Privacy Impact Assessment

for the

Law Enforcement Officers Safety Act Program (LEOSA)

DHS Reference No. DHS/ALL/PIA-087

November 13, 2020

Homeland Security

Abstract

The Law Enforcement Officers Safety Act of 2004 (LEOSA)[1] exempts "qualified law enforcement officers" and "qualified retired law enforcement officers" from most state and local laws prohibiting the carriage of concealed firearms. The U.S. Department of Homeland Security (DHS) and its law enforcement Components have established procedures with respect to qualified retiring, retired, separating, and separated law enforcement officers (LEO) and the application of the relevant provisions of LEOSA. This Privacy Impact Assessment (PIA) documents how DHS collects, uses, and maintains personally identifiable information (PII) of LEOs who apply to carry concealed firearms pursuant to LEOSA.

Introduction

LEOSA exempts qualified LEOs from most state laws prohibiting the carrying of concealed firearms provided that the LEO is carrying photographic identification (LEOSA ID) issued by their (former) employing agency that attests that they meet certain eligibility criteria. DHS policy allows these qualified LEOs to apply for a LEOSA ID that, when all conditions are met, satisfies the requirements of LEOSA. DHS has published a Directive[2] and corresponding Instruction[3] to establish the policy and procedures with respect to qualified retiring, retired, separating, and separated LEOs and the application of the relevant provisions of LEOSA, as amended.

Under LEOSA, qualified LEOs can carry a concealed firearm as long as they carry identification indicating they are former law enforcement officers and proof of up-to-date annual state firearms testing certification. DHS implementation of LEOSA provides that a qualified LEO is an individual who:

(1) Separated from service as a LEO in good standing with DHS;

(2) Before separation, was authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of, any person for any violation of law, and had statutory powers of arrest or apprehension under section 807(b)

[1] 18 U.S.C. § 926C. The Act was introduced during the 108th Congress as H.R. 218 and enacted as Pub. L. No. 108-277. The law was later amended by the Law Enforcement Officers Safety Act Improvements Act of 2010 (S. 1132, Pub. L. No. 111-272) and Section 1099C of the National Defense Authorization Act for Fiscal Year 2013 (H.R. 4310, Pub. L. No. 112-239). It is codified within the provisions of the Gun Control Act of 1968 as 18 U.S.C. §§ 926B and 926C.

[2] LAW ENFORCEMENT OFFICERS SAFETY ACT, DHS DIRECTIVE 257-01 (2017), *available at* https://www.dhs.gov/sites/default/files/publications/mgmt/human-resources/mgmt-dir_257-01-law-enforcement-officers-safety-act_rev-01.pdf.

[3] THE LAW ENFORCEMENT OFFICERS SAFETY ACT INSTRUCTION, DHS INSTRUCTION 257-01-001 (2017), *available at* https://www.dhs.gov/sites/default/files/publications/18_0118-mgmt-dir_257-01-001-law-enforcement-officers-safety-act-instruction.pdf.

of Title 10, United States Code (article 7(b) of the Uniform Code of Military Justice);

(3) Before separation, served as a LEO for an aggregate of 10 years or more; or separated from service as a LEO with DHS, after completing any applicable probationary period of such service, due to a service-connected disability, as determined by DHS;

(4) During the most recent 12-month period, has met, at the expense of the LEO, the standards for qualification in firearms training for active LEOs, as determined by the former agency of the LEO, the state in which the LEO resides, or if the state has not established such standards, either a law enforcement agency within the state in which the LEO resides or the standards used by a certified firearms instructor that is qualified to conduct a firearms qualification test for active duty officers within that state;

(5) Has not been officially found by a qualified medical professional employed by DHS to be unqualified for reasons relating to mental health or has not entered into an agreement with DHS in which the LEO acknowledges he or she is not qualified under this section for reasons relating to mental health;

(6) Is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

(7) Is not prohibited by federal law from receiving a firearm.

DHS uses the applicant's information to verify that the individual meets the criteria for issuance. Components retain the discretion to require individuals to submit supporting documentation and to undergo further vetting. This may include documentation evidencing 10-plus years of law enforcement officer service (e.g., SF-50) or results of up-to-date criminal history checks (e.g., Federal Bureau of Investigation (FBI) National Crime Information Center (NCIC) check). The Component may also conduct a review of the individual's records associated with misconduct, security clearance suspensions and revocations, and psychological fitness for duty. No further checks are conducted once the applicant is approved and receives the LEOSA ID.

LEOSA does not exempt LEOs from other federal laws or regulations, including any restrictions on the carriage of firearms on transportation systems (such as commercial airlines) and does not confer any law enforcement power or authority to use the firearm. Whenever a retired or separated LEO experiences an event which would disqualify him or her from receiving a firearm under 18 U.S.C. § 922, he or she must immediately notify the agency who sponsored the LEOSA ID and certifying state entities.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[4] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[5]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[6] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts PIAs on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[7] and the Homeland Security Act of 2002, Section 222.[8] Given that DHS's implementation of LEOSA is programmatic, rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the FIPPs. This PIA examines the privacy impact of DHS LEOSA programs as they relate to the FIPPs.

1. Principle of Transparency

Principle: *DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.*

DHS published a publicly available Directive and corresponding Instruction establishing DHS's policy with respect to qualified retiring, retired, separating, and separated LEOs formerly in the employ of the Department and the application of the relevant provisions of LEOSA. These policy documents provide information on the responsible entities, procedures, and requirements of the implementation of LEOSA. Notably, each Component is responsible for its own implementation of LEOSA. In accordance with Component-specific procedures, each Component is responsible for making available three documents to its LEOs who have previously retired or

[4] 5 U.S.C. § 552a.
[5] 6 U.S.C. § 142(a)(2).
[6] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[7] 44 U.S.C. § 3501 note.
[8] 6 U.S.C. § 142.

separated from the Component, a law enforcement position in the Component, or a law enforcement position within the Component's predecessor agencies:

1. A copy of the statute (18 U.S.C. § 926C);

2. The factors that would prevent an individual from receiving or possessing a firearm under federal law (18 U.S.C. § 922); and

3. LEOSA Fact Sheet (or similar informational document).[9]

Individuals who wish to carry concealed firearms pursuant to LEOSA must apply on behalf of themselves to their respective Component. This application form includes a Privacy Act statement indicating the authority for the collection, the purpose of collecting the information, how the information may be shared, and that this disclosure of PII is voluntary. However, applicable LEOs will not be able to obtain a LEOSA ID and carry a concealed firearm under this program unless they have submitted all the required information.

Furthermore, this PIA discusses the overall LEOSA process, the types of information collected, redress procedures, and other privacy risks associated with this program. The appropriate SORN, DHS/ALL-023 Department of Homeland Security Personnel Security Management,[10] that covers these records also provides notice.

Privacy Risk: There is a risk that applicants may not know DHS conducts additional checks to determine an applicant's suitability.

Mitigation: The risk is mitigated. Through the publication of this PIA and the notice provided on the LEOSA application form itself, DHS provides sufficient notice that additional checks are required to determine an applicant's eligibility. For example, the Transportation Security Administration (TSA) requires applicants to affirm that they understand TSA will conduct an NCIC check at the time of the application. Alternatively, U.S. Customs and Border Protection (CBP) requires applicants to obtain their own FBI criminal history checks and submit them with their LEOSA application.

2. Principle of Individual Participation

Principle: *DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

[9] For example, *see* U.S. CUSTOMS AND BORDER PROTECTION, CBP LAW ENFORCEMENT OFFICERS SAFETY ACT (LEOSA) FACT SHEET, *available at* https://www.cbp.gov/document/fact-sheets/cbp-law-enforcement-officers-safety-act-leosa-fact-sheet.

[10] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, 85 Fed. Reg. 64511 (October 13, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

The LEOSA application collects information directly from applicants. The individual applicant completes the application, attests to the veracity of its contents, and submits it voluntarily. The individual is provided notice that additional checks may occur by the respective Component to determine the applicant's eligibility (e.g., good-standing, qualified). Once submitted, the respective Component then conducts these necessary checks independent of the applicant. These queries may include an NCIC criminal history check or internal DHS checks, such as checks of personnel records and/or any internal agency reports of investigation or management inquiries that may affect an applicant's fitness to carry a firearm.

An individual submits his or her application directly to a program office responsible for conducting that Component's LEOSA program responsibilities. Individuals can contact that office at any time to correct submitted information. However, DHS presumes the submitted information to be accurate as it is submitted directly by the individual applicant.

In addition, individuals seeking access to or amendment of their records may submit a request in writing to the DHS Chief Privacy and Freedom of Information Act (FOIA) Officer at the below address, or to the respective Component's FOIA officer, which can be found at https://www.dhs.gov/foia-contact-information. DHS also allows Privacy Act and FOIA requests to be submitted electronically at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form.

Chief Privacy Officer and Chief Freedom of Information Act Officer
Privacy Office, Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528

Privacy Risk: There is a risk that inaccurate information could be collected from an individual and not be able to be corrected.

Mitigation: This risk is mitigated. Individuals have the ability to correct their information via the same process by which the information was submitted. Individuals may correct their information at any time during the LEOSA application process. They may also submit a Privacy Act or a FOIA request to the appropriate Component. The LEOSA application form and this PIA provide notice of these correction processes.

3. Principle of Purpose Specification

Principle: *DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

DHS collects PII as part of the LEOSA application process in accordance with 18 U.S.C. § 926C and the DHS LEOSA Directive/Instruction. The information is used to approve or deny the issuance of a LEOSA ID authorizing the individual to carry a concealed firearm pursuant to

LEOSA. The applicant's information is used to verify that the applicant meets the criteria for issuance, including conducting any necessary criminal history record checks or checks of Components records associated with misconduct, security clearance suspensions and revocations, or other issues impacting an individual's fitness to carry a firearm. No further checks are conducted once an applicant is approved and receives the LEOSA ID.

Use of this data is consistent with that listed in this PIA and the applicable SORN, DHS/ALL-023 Personnel Security Management System of Records.

Privacy Risk: There is a risk that information collected from applicants will be used for purposes unrelated to the LEOSA program.

Mitigation: The risk is mitigated. Components limit access of LEOSA applicant information to authorized personnel with a need-to-know. Each Component implements the provisions of LEOSA differently, but maintains applicant information in secure systems, such as access-controlled SharePoint sites or specific systems.[11]

In addition, Components already maintain much of this information collected from retiring, retired, separating, and separated LEO applicants. The information collected is used to determine the eligibility of such an applicant.

4. Principle of Data Minimization

Principle: *DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

Individuals who wish to obtain a LEOSA ID must complete a LEOSA application. A LEOSA application generally collects the following information:

- Name;
- Phone Number;
- Email Address;
- Home Mailing Address;
- Social Security number;
- Date of Birth;

[11] For example, CBP maintains LEOSA information in the Firearms, Armor, and Credentials Tracking System (FACTS). *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE FIREARMS, ARMOR, AND CREDENTIALS TRACKING SYSTEM (FACTS), DHS/CBP/PIA-047 (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

- Entry on Duty/Separation Date;
- Last Office/Location of Record Address; and
- Current or Previous Supervisor's Name, Email, and Office Phone Number.

In addition, supporting documentation may be required to be submitted with the application, such as:

- Digital Passport Photo;
- Documentation evidencing 10+ years of law enforcement officer service (e.g., SF-50);
- Termination SF-50, as appropriate;
- Copy of Driver's License or State Issued Identification Card;
- Self-Attestation that the applicant meets the requirements;
- Self-obtained FBI Summary Check; and
- Signed Authorization to check Agency Records.

The LEOSA application only solicits information that is relevant to making a determination on the individual applicant. To promote data minimization in the application process, Components establish their own methods for the information needed to fulfill the requirements of administering LEOSA, the approval/denial process, and retention of application data.[12] In addition, Components may also collect and maintain information relating to any disqualifying information about an individual that has already received a LEOSA ID.

Privacy Risk: There is a risk that the LEOSA application collects more information than necessary.

Mitigation: The risk is mitigated. Each Component works with its respective Privacy Office on the creation and implementation of the LEOSA application form. During this process, a Privacy Threshold Analysis (PTA) is completed, ensuring that the information collected aligns with the Directive/Instruction, this PIA, and the applicable SORN.

[12] For example, TSA maintains all eligible application packages are covered under NARA Disposition Authority Number DAA-0560-2019-0005-0001 and destroyed after 99 years. All ineligible application packages are covered under NARA Disposition Authority Number DAA-0560-2019-0005-0002 and destroyed after 1 year. *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER DAA-0560-2019-0005-0001, U.S. DEPARTMENT OF HOMELAND SECURITY, LAW ENFORCEMENT OFFICERS SAFETY ACT (LEOSA) PROGRAM (2019), *available at* athttps://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0560/daa-0560-2019-0005_sf115.pdf.

5. Principle of Use Limitation

Principle: *DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

During the process of determining whether the applicant is eligible for a LEOSA ID the application information provided may be shared with other Components and government agencies in connection with the routine uses identified in DHS/ALL-023. Besides this external sharing during the application check process, external sharing is not normally part of the LEOSA application process. However, by way of example only, sharing information with local law enforcement investigating whether the individual was authorized to carry a concealed firearm might be performed under the routine uses of this SORN, which permit disclosure to an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations.

Privacy Risk: There is a risk that records may be shared inappropriately outside of the Department.

Mitigation: The risk is mitigated. Access to LEOSA applicant information is limited to authorized personnel with a need-to-know. Any information shared outside of the Department would be documented in the individual applicant's record or automatically through the use of system logs.

6. Principle of Data Quality and Integrity

Principle: *DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

As information is directly submitted by applicants, DHS assumes that there is a high likelihood that it is correct, to include the required supporting documentation. Individuals attest to the accuracy and correctness of their submitted information on the LEOSA application.

Once submitted, the application and supporting documentation are reviewed for sufficiency. Any incomplete documents result in a denial of the application, with the possibility of resubmission once any deficiencies with the application package are resolved. Depending on the Component's implementation of its LEOSA program, some applications are submitted to an applicant's current or previous supervisor, further providing an opportunity to ensure accuracy of information and ease of correction.

After a package is deemed sufficient, LEOSA program personnel review internal records and conduct any necessary checks to ensure that the applicant meets requirements for issuance of a LEOSA ID, but also to further ensure the individual's submitted information is accurate.

Privacy Risk: There is a risk that inaccurate information could be used by the DHS Component to determine an applicant's LEOSA eligibility.

Mitigation: This risk is partially mitigated. An individual's information is expected to be correct when it is submitted directly by him or her. However, an individual has the ability to correct his or her information via the same process by which the information was submitted. During the DHS Component's review of an applicant's eligibility, it reviews relevant data in other DHS databases or other government agency databases. DHS Components rely on the accuracy measures of those systems to assist with its eligibility determinations.

7. Principle of Security

Principle: *DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

Components have well-established and comprehensive information handling processes in place to enhance information security and eliminate possible misuse, loss, or unintended or inappropriate disclosure of PII. LEOSA application information is maintained on access-controlled SharePoint sites or specific IT systems with strict adherence to access control policies enforced by system or database implementation in coordination with and through oversight by Components' security officers. Access is limited to those with an authorized need-to-know. Further, applicants are requested to password-protect documents upon submission.

8. Principle of Accountability and Auditing

Principle: *DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

Components may implement periodic audits to ensure continued compliance with privacy and security requirements. Chiefly though, access to LEOSA applicant information is approved specifically for, and limited only to, users who have an official need for the information in the performance of their duties. All DHS personnel are required to complete annual information security and privacy training covering their responsibility to secure and protect sensitive information and PII.

Conclusion

LEOSA is a federal law enacted in 2004, which exempts qualified LEOs from most state

and local laws prohibiting the carriage of concealed firearms as long as the individual has LEOSA-compliant photographic identification along with valid annual state firearms training documentation. DHS implements LEOSA through its Directive/Instruction and the individual Components are responsible for managing their own program. Through coordination with its respective Privacy Office, each Component implements its LEOSA responsibilities while protecting privacy and ensuring mitigation of any significant risks.

Approval Signature

Original, signed version on file with the DHS Privacy Office.

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717