Privacy Impact Assessment
for the

Homeland Security Information Network Leveraging Military Training Portal

DHS/ALL/PIA-062

June 19, 2017

Contact Point
Ronald M. Salazar
DHS Senior Advisor to the Office of the Secretary of Defense and the Joint Staff
DHS Office of the Military Advisor
(703) 697-3630

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), in close collaboration with Department of Defense (DoD) partners, has designed the Leveraging Military Training (LMT) Portal, built on the Homeland Security Information Network (HSIN) platform, in order to enable DHS to share information with DoD relating to law enforcement needs and activities. Many DHS initiatives, programs, and operations require collaboration and communication among affected officials and stakeholders. The establishment of the LMT Portal is one way DHS and DoD have effectuated such collaboration, allowing authorized users to obtain, post, and exchange information, access common resources, and perform general communication and coordination with homeland security enterprise partners. DHS is conducting this Privacy Impact Assessment (PIA) to document and provide transparency about the LMT process, and to highlight the information that will be collected within the LMT Portal to facilitate collaboration between DHS and DoD and to provide accountability to Congress and the public.

Introduction

Over the last decade, the Department of Defense (DoD) has provided considerable support to the Department of Homeland Security (DHS) in securing our Nation's borders. In support of this collaboration, on December 23, 2016 Congress enacted Section 1014 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2017 (Pub. L. 114-328). The provision requires DHS to identify and communicate to the Secretary of Defense the information needs of the Department relating to law enforcement activities in proximity to the international borders of the United States. DoD will in turn use this information to plan for and conduct military training that provides incidental benefit to DHS border security efforts through the sharing of information between DoD units and elements of DHS.

Specifically, legislative language in the FY 2017 NDAA directs that no later than June 20, 2017, the Secretary of Homeland Security, in coordination with the Secretary of Defense, will establish a "formal mechanism," through which DHS information needs are identified and communicated to DoD. The LMT Portal serves as the formal mechanism, or information sharing platform, to meet congressional intent for DHS to engage in LMT activities with DoD.

LMT is not a new concept or authority. Section 271 (formerly Section 371) of Title 10 U.S. Code (U.S.C.), *Use of Information Collected During Military Operations,* states that the Secretary of Defense may, in accordance with other applicable law, provide to federal, state, or local law enforcement officials any information gleaned during the normal course of military training or operations that may be relevant to a violation of any federal or state law within the jurisdiction of such officials. This authority, in law since 1981, is codified and formalized by

DoD within its LMT Initiative. DoD has supported DHS using LMT authorities over the years through localized and/or ad-hoc efforts coordinated at the field level.

The following example is illustrative of a typical LMT activity between DHS and DoD, at the local level. Within the San Diego area of Southern California, the nation faces an escalating homeland security threat of high-speed "Panga" boats employed by criminal organizations, conveying a spectrum of illicit loads ranging from drugs to illegal migrants to other potentially more dangerous threats. Emanating from Mexico, these boats circumvent law enforcement and customs regimes by traveling northward through the Eastern Pacific, with the ultimate intent of delivering their illicit payloads farther north along the California coast. Per coordination between military commanders and homeland security officials at the local level, U.S. Navy helicopters performing military proficiency training offshore routinely communicate sightings of potentially illicit maritime traffic to U.S. Coast Guard (USCG) and U.S. Customs and Border Protection (CBP) Air & Marine Operations units in real-time, so that these law enforcement agencies are cued to investigate and effect appropriate law enforcement action to counter these threats to our national security.

LMT allows DoD units - as they conduct training in proximity to U.S. international borders and the approaches to the homeland[1] - the ability to pass actionable law enforcement-related information in real-time to DHS Components. LMT is a way of operationalizing the homeland security campaign, "If You See Something, Say Something," between DHS and DoD. In doing so, DHS may leverage DoD capability and capacity where and when needed to reinforce DHS border security efforts, at no additional cost to DoD or the American taxpayer, as DoD delivers this support in a manner incidental to its training activities already funded by Congress.

In response to congressional intent, DHS and DoD are formalizing policy, process, and procedure for routinizing LMT activities through the LMT Portal. DHS has developed an LMT Lifecycle Model, explained below, to orchestrate how LMT activities will be conducted between DHS and DoD.

DHS will define and communicate its law enforcement information needs to DoD by developing and posting "DHS Opportunities" - a single homeland security capability need within a defined geographic area and domain (Air, Land, and/or Maritime), as codified by a DHS Component - within the LMT Portal.[2] Each DHS Opportunity will be rigorously reviewed and

[1] Each DHS Component relies on a tailored definition of "proximity to the border" based on its unique law enforcement authorities, mission, and the scope of its operational responsibilities.

[2] DHS Components - such as USCG, CBP, and U.S. Customs and Immigration Enforcement (ICE) - will document their unique law enforcement capability needs within the LMT Portal via pre-configured templates, tailored to Land, Air, and Maritime domains. "DHS Opportunities" will include many of the same activities - for example, air and maritime surveillance and engineering support - on which DHS and DoD have been routinely collaborating for the past 25 years through DoD's Counter Narcotics Program, funded each year by congressional appropriation, under

vetted by DHS leadership. Each DHS Opportunity will, by design, undergo a thorough legal, public affairs, civil rights/civil liberties, and privacy review as part of the approval process, to ensure compliance, sufficiency, and transparency in these functional areas. After the DHS Opportunity is processed through a series of reviews, it will be posted within the LMT Portal on the Homeland Security Information Network (HSIN),[3] where DoD partners may consider supporting it as they plan their annual Mission Essential Task List (METL) military proficiency training.

As the military services plan and forecast their METL training for each year, DoD trainers and commanders will be afforded read-only access to the LMT Portal to consider and select DHS Opportunities, on an elective and discretionary basis. Once a military unit has elected to perform a DHS Opportunity, that unit training officer or commander will reach out to the DHS point of contact for the DHS Opportunity and will conduct coordination activities - outside of the LMT Portal via phone or email - and schedule the LMT training evolution.[4]

After a DoD training evolution has been conducted, it is incumbent upon DHS points of contact to document all results/outcomes for each evolution within the LMT Portal for purposes of reporting, accountability, and transparency, given DoD only has read-only capability within the LMT Portal.

As directed by Congress, DHS will record high-level outcomes of LMT collaboration efforts, to include information such as the number of DHS arrests, illegal material seizures, and/or criminal organization disruptions associated with each LMT training evolution.[5] Specific DHS law enforcement case information, to include personally identifiable information (PII) and data resulting from LMT training evolutions, will not be entered into the LMT Portal, but instead, will be maintained in separate, proprietary law enforcement case systems and databases, routinely used by DHS in the normal course of conducting border security operations.[6] Each DHS Opportunity record will have a data field to reference the appropriate DHS law enforcement case number, in order to safeguard and compartmentalize related law enforcement information outside of the LMT Portal. PII collected by DHS law enforcement agencies as a result of an LMT training evolution will never be entered into the LMT Portal, nor is it ever

---

the auspices of policy and priorities developed by the White House Office of National Drug Control Policy.

[3] The Homeland Security Information Network (HSIN) is a web-based platform, run by DHS, which is designed to allow federal, state, local, tribal, and territorial government agencies to share "Sensitive But Unclassified (SBU)" information with each other over a secure channel.

[4] A DoD LMT training evolution is defined as a single DoD training iteration or event in response to a DHS Opportunity, conducted over a defined period of time and performed by a single, unique DoD element.

[5] DHS law enforcement generally refer to these statistics holistically as "end game" outcomes, resulting from interdiction operations.

[6] For example, if during its offshore military proficiency training a U.S. Navy helicopter sights potentially illicit maritime traffic, it would communicate that information to CBP. All law enforcement actions and data (to include an individual's PII) taken during the resulting CBP investigation/interdiction would be recorded and stored in the CBP system of record, not the LMT Portal.

shared with DoD.

LMT is not intended to "militarize the border." While conducting LMT training evolutions, DoD units will never engage in law enforcement activity. DoD will not conduct any type of arrest or seizure, or have contact with individuals suspected of illicit activity. All information related to suspected illicit activity will be passed to a DHS law enforcement official charged with the authorities to perform law enforcement.[7] It is incumbent on the DHS law enforcement official to determine the level of response to suspected illicit activity and determination of any violation of law. All LMT-related support provided by DoD units will be performed within conditions and parameters reviewed and approved by DHS Component and functional area leadership. DoD will not retain any records for individual LMT training evolutions or collect any PII.

Congressional guidance requires DHS and DoD to report the results of LMT collaborative activities annually. To that end, DHS will report to Congress on data statistics reflecting end game outcomes and overarching law enforcement results[8] achieved through incidental collaboration with DoD partners.

The PII that will be shared on the LMT Portal will be limited to contact list information for the purposes of coordinating DoD training to support DHS Opportunities. This information will be provided voluntarily by DHS and DoD participants in the LMT Portal on HSIN. Contact information such as name, official title, business email, and business phone will be collected from DHS and DoD points of contact for the sole purpose of coordination between those two entities to fulfill the mission of the LMT Portal. Contact information is not used for any purpose other than to enable contact outside of HSIN via phone or email to enable collaboration and coordination between the two points of contact.[9]

---

[7] The level of coordination and selection of methods of communication - radio, phone, email, etc. - will be arranged between DoD unit commanders and DHS law enforcement officials as they perform planning and coordination for discrete evolutions. No passing of information will ever occur via the LMT Portal, as DoD only has read-only capability.

[8] Details on reporting can be found in Section 1014(d)(2) of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2017 (Pub. L. 114-328), which requires DHS to report to the congressional defense committees, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate.

[9] The information collected to register and gain access to HSIN is outlined by DHS/ALL/PIA-061-1 HSIN Release 3 User Accounts, *available at* https://www.dhs.gov/privacy. The risks associated with the contact information that individuals voluntarily provide is outlined in DHS/ALL/PIA-006 DHS General Contacts List, *available at* https://www.dhs.gov/privacy.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 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.

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. 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 Privacy Impact Assessments (PIA) on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. Given that LMT is an initiative rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Principles. This PIA examines the privacy impact of LMT operations as it relates to the Fair Information Principles.

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. There should be no system the existence of which is a secret.

The PII that will be shared on the LMT Portal will be limited to DHS and DoD employee business contact list information for the purposes of coordinating DoD training to support DHS Opportunities. This information will be provided voluntarily by DHS and DoD participants directly in the LMT Portal.[10] Contact information such as name, official title, business email, and business phone will be collected from DHS and DoD points of contact for the sole purpose of coordination between those two entities to fulfill the mission of the LMT Portal. Contact information is not used for any purpose other than to enable contact outside of HSIN via phone or email to enable collaboration and coordination between the two points of contact. Notice of this

[10] As DoD members have read-only access to the LMT Portal, their contact information will be input by DHS Opportunity points of contact (POC). The DoD POC will respond to evolutions by contacting the DHS POC. The DHS POC will then input contact information provided by the responding DoD POC.

information being collected by DHS is provided to the individual at the time of collection through HSIN.[11]

DHS is not collecting PII from members of the public or posting it on the LMT Portal. DoD is also not collecting any PII, and does not relay any PII when it informs the appropriate DHS law enforcement official of suspected illicit activity. This PIA provides notice to members of the public of the DoD/DHS collaboration in proximity of the U.S. border. Because of the geographical location of the LMT training evolutions, U.S. citizens may be impacted even though no PII is being collected.[12]

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.

The inclusion of PII (government employee/military member name, official title, business phone, and business email address) is entirely voluntary and with the full understanding by all individuals involved in the LMT Portal on how the information is to be used. When individuals register for a HSIN account they are provided with information on how their PII will be used.[13]

Information that DoD relays to DHS (such as the GPS coordinates for the sighting of suspected illicit activity) could result in a DHS encounter with an individual in which PII is subsequently collected. The privacy risks of DHS collecting that information would be outlined in other DHS privacy compliance documentation. For example, if CBP encountered individuals trying to illegally cross the border based on the GPS coordinates relayed by DoD, CBP would then collect PII from the individuals. The information collected during the encounter would be covered by a CBP-specific System of Records Notice (SORN).[14]

---

[11] For more information, please see DHS/ALL/PIA-061-1 HSIN Release 3 User Accounts, *available at* https://www.dhs.gov/privacy. This PIA outlines the privacy risks of the information that is collected from individual users in order to grant them access to HSIN and the information shared on HSIN.

[12] For example, DoD may inform DHS of suspected illicit activity that is taking place on the property of a private sector land owner. In this case, the U.S. Border Patrol (USBP) may respond to the suspected illicit activity. However, for LMT activities, the USBP Special Coordination Center in El Paso, Texas, will have pre-cleared and coordinated all land use rights and permissions with private sector land owners, and other federal, state, local, tribal, and territorial legal authorities as necessary, prior to DHS personnel providing support.

[13] For more information about this process, please *see* DHS/ALL/PIA-061-1 HSIN Release 3 User Accounts, *available at* https://www.dhs.gov/privacy. The collection of this information to register for HSIN is covered by DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).

[14] In this example, the applicable privacy compliance documentation is as follows: DHS/CBP-023 Border Patrol

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.

The information that is collected on the LMT Portal from DoD and DHS personnel is governed by the HSIN LMT Charter and the DHS LMT Concept of Operations (CONOPs). These documents serve to provide policy, authority, and operational guidance for the implementation of LMT within DHS. Both documents reflect explicit business rules for the specific use and application of PII. The contact PII collected from DoD and DHS personnel is not used for any purpose other than access to HSIN and to enable contact outside of HSIN via phone or email to enable collaboration and coordination between DHS and DoD points of contact. This limited amount of contact PII restricts the ability to use it for anything other than its intended purpose.

In the course of DoD training evolutions, all information related to suspected illicit activity will be passed to an appropriate DHS law enforcement official. DoD will not collect any PII during its training evolutions.

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).

In order for DoD to assist DHS in performing its law enforcement responsibilities, it must share relevant information. However, DoD and DHS have determined that no PII (other than the voluntarily-provided contact information for the purposes of contact other members of the LMT Portal) is necessary to carry out this mission.

The LMT Portal will only be a repository for contact PII as described above - there is no intent to ever exceed the minimal PII requirement envisioned for purposes of coordinating LMT activities between DHS and DoD. Information within the LMT Portal is governed by provisions articulated within the HSIN LMT Charter, which adhere to all applicable DHS records disposition schedules.

Enforcement Records (BPER), 81 FR 72601 (October 20, 2016), which allows for the record of the detection, location, encounter, identification, apprehension, and/or detention of individuals who commit violations of U.S. laws enforced by CBP or DHS between the ports of entry.

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.

DoD and DHS have determined that no member of the public's PII is necessary to coordinate activities through the LMT Portal. DoD will only share non-PII data (*e.g.*, location information, suspected illicit activity descriptions) with DHS during the course of LMT evolutions. In turn, DHS will not share any PII information back to DoD. The only information DHS shares back to DoD is through the LMT Portal and documents the results/outcomes (*e.g.*, arrests, illegal material seizures) for each LMT training evolution for purposes of reporting, accountability, and transparency.

Per process and procedure deliberately embedded within the design of the LMT Portal, PII will only be used as described in the HSIN LMT Charter and DHS LMT CONOPs. These documents explain that the PII maintained and shared on the LMT Portal will be voluntarily collected from DoD and DHS points of contact for the sole purpose of coordination between those two entities to fulfill the LMT mission.

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.

The LMT Portal is only used as a repository for the limited business contact information collected. Personnel voluntarily provide the information and individuals may correct inaccurate or erroneous contact information at any time through HSIN. As DoD personnel have read-only access, a DHS POC is required to correct or amend any DoD personnel contact information.

Privacy Risk: There is a risk that the LMT Portal may hold incorrect contact information on DoD personnel because they do not directly input the information.

Mitigation: This risk is mitigated by allowing DHS personnel the ability to update and correct DoD POC information at any time. DoD POCs only need to contact DHS POCs to have the information updated.

Privacy Risk: As part of the overall LMT Initiative, there is a risk that DoD may pass inaccurate information to DHS, upon which DHS then acts.

Mitigation: This risk is mitigated. The goal of this initiative is for DoD to pass information related to suspected illicit activity to DHS in order to perform law enforcement responsibilities. This information may not always be accurate. However, because none of this information will

contain PII and DoD and DHS have minimized the amount of information needed to carry out the LMT mission, there are minimal impacts to privacy. Additionally, DHS will not use information received from DoD as its sole means to take a law enforcement action against an individual.

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.

By design, in order to maintain high standards of security compliance, all individuals requesting access to the LMT Portal will require nomination and validation for identity confirmation and admittance permissions for a HSIN account.[15] Subsequently, all users will undergo a secondary screening for "need-to-know" and access into the LMT Portal.

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.

By design, the LMT Portal will not collect PII (other than limited business contact information that which is voluntarily provided by DoD and DHS personnel) and is the primary way in which DoD and DHS will ensure information is used in accordance with the stated practices. Additionally, the HSIN LMT Charter and DHS LMT CONOPs ensure awareness, accountability, and compliance of what information should and should not be shared.

As a business rule and process safeguard, the DHS Office of the General Counsel (OGC), DHS Privacy Office (PRIV), Office for Civil Rights and Civil Liberties (CRCL), and Office of Public Affairs (OPA) will be granted full administrative rights to the LMT Portal for the purpose of full transparency and accountability. Each functional area office will have the ability to perform audits within their area of equity at all times.

Further, all DoD and DHS users of the LMT Portal will be required to successfully pass HSIN's PII training.

[15] For more information about the HSIN nomination and validation process, please *see* DHS/ALL/PIA-061-1 HSIN Release 3 User Accounts, *available at* https://www.dhs.gov/privacy.

Conclusion

The LMT effort between DHS and DoD shows great potential to enhance the nation's border security posture. All efforts have been made in the development of the policy, process, and procedures for formally conducting LMT activities at the Departmental level between DHS and DoD and in the design of the HSIN LMT Portal to ensure the FIPPs have been considered and standards have been met. This PIA provides transparency to all homeland security stakeholders, to include the public, on how DHS intends to implement the statutory requirement to leverage military training.

Responsible Officials

Ronald M. Salazar (SES)
DHS Senior Advisor to the Office of the Secretary of Defense and the Joint Staff
Office of the Military Advisor to the Secretary, DHS

Approval Signature

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

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security