Privacy Compliance Review

of the

ICE Pattern Analysis and Information Collection Law Enforcement Information Sharing Service

December 15, 2011

Contact Point
James Dinkins
Executive Associate Director, Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

I. SUMMARY

The U.S. Government Accountability Office (GAO) recently conducted a review of the selected DHS systems that support counterterrorism including the U.S. Immigration and Customs Enforcement Pattern Analysis and Information Collection System (ICEPIC) Law Enforcement Sharing (LEIS) Service.[1] GAO's review found that the LEIS Service was not described in the Privacy Impact Assessment (PIA) that was approved for the ICEPIC system in January 2008.[2] Given E-Government Act and DHS policy requirements for conducting PIAs, GAO recommended that the Chief Privacy Officer investigate whether the LEIS component of ICEPIC should be deactivated until a PIA that includes this component was approved. DHS concurred with the recommendation and as a result of the report findings and recommendations, the DHS Privacy Office initiated this Privacy Compliance Review (PCR).[3]

ICEPIC is a toolset that assists the U.S. Immigration and Customs Enforcement (ICE) law enforcement agents and analysts in identifying suspect identities and discovering possible non-obvious relationships among individuals and organizations that are indicative of violations of the customs and immigration laws as well as possible terrorist threats and plots. The LEIS Service allows external law enforcement officers (federal, state, local, tribal and international partners) direct access to certain DHS law enforcement data sources compiled by ICEPIC. The objectives of our review were to 1) identify the cause of the privacy compliance gap regarding the LEIS Service and 2) evaluate whether the compliance gap warranted a deactivation of the LEIS Service until the PIA could be approved.

To address our objectives, we reviewed the GAO report and associated recommendation, ICEPIC privacy documentation, program documentation, and Memoranda of Agreement (MOAs) in place with ICE sharing partners for the LEIS Service. We also conducted interviews with the ICE Privacy Officer, as well as with ICE Executive and Deputy Directors for the DHS Law Enforcement Sharing as part of the PIA update process. Our review began in September 2011 with GAO's identification of the compliance gap and recommendation to us and was concluded in November 2011. The PIA update to ICEPIC fully describing the LEIS Service published on October 27, 2011[4] and obviated the need to deactivate the Service, but

---

[1] GAO, *Data Mining: DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism,* GAO-11-742, (Washington, D.C.: September 2011).

[2] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_icepic.pdf.

[3] The DHS Privacy Office exercises its authority under Section 222 of the Homeland Security Act to assure that technologies sustain and do not erode privacy protections through the conduct of PCRs. Consistent with the Privacy Office's unique position as both and advisor and oversight body for the Department's privacy sensitive programs and systems, the PCR is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation.

[4] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_icepic-4a.pdf.

we completed the PCR in order to examine the factors that led to the Chief Privacy Officer's decision to direct an expedited preparation and approval of the PIA.

Our review found that, although the original PIA published in January 2008 accurately described ICEPIC at the time of its publication, the subsequent addition of the LEIS Service to ICEPIC should have triggered a PIA update. A PIA update was not initiated as a result of an incorrect determination in April 2008 by the DHS Privacy Office. Further, this determination was not formally documented in a Privacy Threshold Analysis (PTA). Since GAO made its recommendation to the DHS Privacy Office, a PIA update published that fully describes the LEIS Service. In addition, since 2008, the DHS Privacy Office has taken a number of steps to strengthen its compliance processes, reducing the likelihood of a similar compliance gap. While the publication of the ICEPIC PIA Update obviated the need to deactivate the LEIS Service, the facts uncovered during this PCR and the PIA update process validate that directing the expedited preparation and review of the PIA was an appropriate remedy given the nature of the compliance gap, the privacy impact, and mitigating factors such as ICE oversight mechanisms in place governing the LEIS Service. Further, the sharing taking place under the LEIS Service continued to have an accurate System of Records Notice (SORN) in place containing an appropriate routine use, in compliance with the Privacy Act of 1974. By directing the expedited preparation and review of the PIA update, the DHS Privacy Office was able to work with the program to bring it into compliance with the E-Government Act and DHS policy.

While we believe the ICEPIC PIA Update published on October 27, 2011 and this PCR address the GAO's recommendation, this PCR highlighted the need for criteria that evaluate and remedy compliance gaps in a manner that upholds privacy and DHS operational needs. Accordingly, we are recommending the development of specific evaluation criteria and remedies to aid the Chief Privacy Officer when areas of non-compliance are identified. The DHS Privacy Office is currently developing these criteria to aid its decision-making in the future.

II. SCOPE AND METHODOLOGY

In September 2011, the DHS Privacy Office initiated a PCR in response to the GAO findings and recommendations regarding the ICEPIC LEIS Service. The PCR was led by Rebecca Richards (Director of Privacy Compliance), Jamie Danker (Associate Director of Privacy Compliance) and Shannon Kelso (Privacy Compliance Specialist). Lyn Rahilly (ICE Privacy Officer), Steven Cooper (ICE Executive Director, DHS Law Enforcement Sharing Initiative), and Jason Henry (ICE Deputy Director, DHS Law Enforcement Sharing Initiative) through their work on the ICEPIC PIA Update participated in the review. The DHS Privacy Office conducted the following activities to address our objectives:

- Identified the current state of the ICEPIC LEIS Service and compared it against the original 2008 ICEPIC PIA.
- Evaluated whether the 2008 ICEPIC PIA met E-Government Act of 2002 and DHS policy requirements for conducting PIAs.
- Reviewed the initial 2007 ICEPIC Privacy Threshold Analysis (PTA).
- Reviewed the DHS/ICE-002 ICE Pattern and Analysis and Information Collection (ICEPIC) SORN (August 18, 2008, 73 FR 48226) to determine if the sharing taking place through the LEIS Service had an appropriate routine use in place as required under the Privacy Act of 1974.
- Interviewed the ICE Privacy Officer, the ICE Executive Director for the DHS Law Enforcement Sharing Initiative, and the ICEPIC Program Manager regarding the compliance gap and the current state of the LEIS Service as part of the process for reviewing the ICEPIC PIA Update.
- Reviewed the standard Memorandum of Agreement (MOA) in place with LEIS Service sharing partners to identify whether privacy protective controls were in place that addressed the DHS Fair Information Practice Principles (FIPPs,) such as use limitation, data minimization, and purpose specification.[5]
- Reviewed LEIS Service program documentation including a set of Frequently Asked Questions (FAQs) about the LEIS Service and the DHS Law Enforcement Information Sharing Initiative, as well as documentation on the specific data elements that DHS shares with external law enforcement partners through the LEIS Service.

III. PRIVACY COMPLIANCE REVIEW

Compliance Documentation

Requirements: Section 208 of the E-Government Act of 2002 (Public Law 107-347) requires agencies to conduct a PIA before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or initiating a new collection of information that will be collected, maintained, or disseminated using information technology. Office of Management and budget (OMB) Memorandum 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, identifies specific PIA triggers, including changes to internal data flows or collections.[6] Specifically, OMB M-03-22

[5] See *DHS Privacy Policy Guidance Memorandum 2008-1, The Fair Information Practice Principles: Framework for Privacy Policy at DHS* (Dec. 29, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[6] http://www.whitehouse.gov/omb/memoranda_m03-22/.

requires a PIA "[w]hen alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form." DHS PIA guidance mirrors E-Government Act and OMB guidance requirements. DHS also requires that PIAs be reviewed and updated as appropriate every three years.[7]

Review: We reviewed the GAO Report and findings, the initial 2007 ICEPIC PTA submission, the ICEPIC PIA from 2008, the DHS/ICE-002 ICEPIC SORN and the standard LEIS Service MOA in place with sharing partners. We also had discussions with the ICE Privacy Officer, who joined ICE shortly after ICEPIC's initial deployment in January 2008. We also interviewed the ICE Executive and Deputy Directors for the DHS Law Enforcement Information Sharing Initiative as part of the ICEPIC PIA update process. We reviewed the 2008 ICEPIC PIA against the current state of the LEIS Service, and the DHS/ICE-002 ICEPIC SORN to determine whether an appropriate routine use was in place for the sharing taking place through the LEIS Service.

Findings: In 2007, ICE completed a PTA for the ICEPIC system which was appropriately adjudicated by the DHS Privacy Office as requiring the completion of a PIA. ICE addressed this requirement with the preparation and approval of a PIA in January 2008 which accurately described ICEPIC at that time. In May 2008, the ICEPIC program requested that the ICE Privacy Officer review and clear on an LEIS Service MOA with a sharing partner. This prompted the ICE Privacy Officer, who had just joined the organization in April 2008, to seek guidance from the DHS Privacy Office on whether a PIA or PIA update to ICEPIC would be required. The DHS Privacy Office made an incorrect determination at that time and did not require the PIA update to be completed. This determination was not formally documented in a PTA. The ICE Privacy Officer noted that the ICE Deputy Director for the DHS Law Enforcement Sharing Initiative was planning to make changes to ICEPIC in the near future that would require an update to the ICEPIC PIA and had planned on describing the LEIS Service in that update for public transparency. However, the planned changes were never implemented, thus the PIA update did not occur, resulting in a compliance gap with regard to notice.

The LEIS Service remained in compliance with the Privacy Act from the onset as an appropriate routine use permitting external sharing with law enforcement partners was in place in the relevant SORN. Specifically, routine use H in DHS/ICE-002 permits sharing "[t]o an appropriate Federal, State, tribal, local, or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related

[7] See *DHS Privacy Policy Guidance Memorandum 2008-2, DHS Policy Regarding Privacy Impact Assessments* (Dec. 30, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence, but only when the disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure."

The DHS Privacy Office acknowledges its error and since the GAO review an update to the ICEPIC PIA published on October 27, 2011. Since 2008, the DHS Privacy Office has made improvements to its compliance processes that will lessen the probability of a recurrence. First, DHS has placed Privacy Officers in the seven major operational components including ICE. The component privacy officers provide DHS components a day-to-day operational level expert who is quickly able to identify privacy risks and mitigation strategies. Since joining ICE in 2008, the ICE Privacy Officer has improved the agency's percentage of the number of IT systems with a valid PIA in place from 17 percent to 80 percent at the end of FY 2011. DHS has also improved its process for reviewing updates to systems and programs, via its PTA process. The PTA is a tool for program managers to propose program changes that allow the component privacy officers and the DHS Privacy Office to analyze the privacy risks and determine next steps. Additionally, DHS has a policy to review PTAs and PIAs every three years. The systematic review of all PTAs and PIAs every three years provides an opportunity to ensure the privacy compliance documentation accurately reflects the operational program. Finally, the DHS Privacy Office has commenced periodic PCRs to confirm compliance and throughout the lifecycle of certain high profile DHS systems.

Evaluation and Remediation of the Compliance Gap

Requirement: As recommended in the GAO report, the Chief Privacy Officer should investigate whether the LEIS Service should be deactivated until such time as a PIA can be completed.

Review: We conducted this PCR to identify causes for the compliance gap and evaluate whether the gap warranted deactivation of the LEIS Service. A PIA Update to ICEPIC fully describing the LEIS Service published on October 27, 2011, and obviated the need to deactivate the Service. We continued our PCR, however, and examined the factors that led to the Chief Privacy Officer's decision to direct an expedited preparation and approval of the PIA. We evaluated the nature of the LEIS Service's privacy compliance gap, the privacy impact, and mitigating factors such as internal oversight mechanisms in place within the program. We also reviewed the standard MOA in place with law enforcement sharing partners to identify whether they addressed key privacy principles such as data minimization, use limitation, and purpose specification.

Findings: Through the course of the PCR and PIA update process, a number of factors were identified that led the Chief Privacy Officer to determine that an

expedited preparation and review of the PIA was appropriate remediation. First, we evaluated the nature of the compliance gap. As previously noted, the introduction of the LEIS Service to ICEPIC without an update to the original PIA resulted in a notice gap with respect to E-Government Act requirements, but the sharing taking place through the service remained in compliance with the Privacy Act. ICE has been forthcoming about the LEIS Initiative and its plans for the LEIS Service during several internal DHS meetings of the Information Sharing Coordination Council[8] (ISCC) as well as in public settings.

We also identified a number of privacy-protective measures that were in place through the use of MOAs with law enforcement sharing partners that mitigated the privacy impact presented by the PIA notice gap. The MOAs addressed FIPPs such as data minimization, purpose specification, and use limitation. Regarding data minimization, the MOAs appropriately restricted law enforcement sharing partners' access to ICEPIC data to only a specific subset of law enforcement data. Information that is restricted from disclosure by statute, regulation or policy is filtered and not shared with these external partner agencies. Regarding purpose specification and use limitation, the information provided through the LEIS Service both to law enforcement partner agencies and DHS ICEPIC users was appropriately limited for use only for official criminal law enforcement purposes, national or homeland security purposes, and for background checks on applicants seeking employment with member agencies. For example, the information may be used to assist with investigations, to notify requesting officials of past criminal behavior, or to validate a subject's key biographic information. Per the MOAs, DHS information accessed by law enforcement sharing partners through the LEIS Service cannot be accessed or used for any other purpose, including general licensing and eligibility for federal or state benefits. In addition, both the DHS Privacy Office and the ICE Privacy Officer reviewed and cleared on agreements through the ISCC process for reviewing information sharing access agreements. In light of these privacy-protective measures and the incorrect guidance given by our office in 2008, the Chief Privacy Officer determined that the expedited completion of the ICEPIC PIA Update was an appropriate remediation strategy.

IV. CONCLUSIONS AND RECOMMENDATIONS

After reviewing the timeline of events, it is clear that our office made an incorrect determination in 2008 regarding the need to update the original ICEPIC PIA. Furthermore, incorrect determination or not, any determination should have been

[8] The ISCC supports the Information Sharing Governance Board, the senior steering committee and policy-making body for information sharing practices at DHS, by developing policy recommendations and guidance. The ISCC reviews all DHS Information Sharing Access Agreements before the agreements become final. As action officers of the ISCC, senior members of the DHS Privacy Office participate in those reviews to ensure the agreements comply with DHS privacy policies, including ISCC guidance, and provide feedback and guidance on incorporating privacy protections into information sharing agreements become final.

appropriately documented using a PTA. The DHS Privacy Office believes that significant improvements in the compliance process made since 2008 that will reduce the risk of this happening again. We concurred with the GAO recommendation at the time and took immediate steps to address it through the expedited preparation of the ICEPIC PIA Update. Further, the Department has worked diligently to improve its privacy compliance and reached its 80 percent target for privacy sensitive systems covered by a valid PIA in FY 2011. ICE also hit the 80 percent target this year for PIAs and since the addition of the ICE Privacy Officer in 2008, has improved ICE's PIA score by 63 points, highlighting the value of component privacy officers.

Although the publication of the PIA update on October 27, 2011 obviated the need to suspend the LEIS Service, this instance nonetheless highlights challenges the Chief Privacy Officers and Chief Information Officers face across the government when policy violations are brought to light. Suspending an operational system is not a decision to be taken lightly. The DHS Privacy Office considered a number of factors when determining that expedited review of the PIA was an appropriate remedy. In absence of the significant oversight mechanism in place through use of MOAs that were reviewed and cleared by both DHS and ICE Privacy Offices through the ISCC process for reviewing information sharing access agreements, an expedited preparation and review of the PIA may not have been the appropriate remedy. As a result of this PCR, DHS has determined that evaluation criteria and remedies for resolving privacy compliance gaps is necessary to aid the Chief Privacy Officer in the future when policy compliance gaps are brought to light. The DHS Privacy Office is currently working on developing these criteria and remedies.

V. PRIVACY COMPLIANCE REVIEW APPROVAL

Responsible Official
James Dinkins
Chief, Current Operations
Executive Associate Director, Homeland Security Investigations
U.S. Immigration and Customs Enforcement

Approval Signature

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security