DHS Privacy Compliance Reviews Open Recommendations as of May 6, 2020

	PCR Name	Component Lead(s)	Date PCR Issued	Recommendation Number	Recommendation Text	Implementation Status
1	U.S. and E.U. Passenger Name Record Agreement	CBP	6/26/2015	9	Given office restructuring and reorganizing within CBP, DHS Office of Policy, DHS Privacy Office, and DHS TRIP, the 2013 CBP PNR Directive should be promptly updated to reflect responsibilities for each office.	Not Implemented
2	U.S. Secret Service	USSS	7/21/2017	2	USSS should formalize and empower the USSS Personally Identifiable Information (PII) Working Group to address privacy shortcomings and implement privacy best practices. ***Note recommendation modified to reflect the goal of formalizing the USSS Privacy Office compliance and oversight responsibilities (not limited to the PII Working Group) and increased engagement across USSS.	Partially Implemented
				3	USSS should formalize the USSS Privacy Officer's authority within decision making fora, such as the Enterprise Governance Council (EGC) and the Information Technology Review Committee (ITRC), where privacy equities can be fully addressed before USSS makes operational decisions.	Partially Implemented
				6	As a best practice, USSS should focus on understanding and implementing standing DHS Privacy Policies, Directives, and Instructions, unless said privacy policies/instructions need to be tailored to USSS. USSS should, however, use appropriate means to raise awareness and oversee implementation and compliance with DHS privacy policies/instructions.	Partially Implemented
				7	USSS should promote privacy Standard Operating Procedures (SOP) among system users and imbed SOPs within privacy sensitive systems.	Partially Implemented
				8	USSS Privacy Office should improve processes and increase oversight of USSS compliance with federal privacy laws, regulations, and DHS privacy policies. This improvement includes timely submission of privacy compliance documents on all privacy sensitive systems/programs/operations.	Partially Implemented
				10	USSS Privacy Office should ensure it supports USSS implementation of DHS Directive Number: 262-05 regarding Information Sharing and Safeguarding by proactively applying appropriate governance mechanisms in the development of information sharing arrangements and ensuring all agreements have been reviewed by the USSS Privacy Office and include all required privacy compliance documents. USSS should ensure the DHS Privacy Office reviews and approves all information sharing and access agreements, as appropriate, to determine if they comply with applicable privacy law and adequately protect individuals' privacy.	Not Implemented
				11	USSS Privacy Office should work with USSS CIO and system and program managers to develop and conduct regularly scheduled user access audits on all privacy sensitive systems to determine if a user has a continued need to know and remove access for those that do not. Users should be required to complete annual privacy training and affirm knowledge of relevant privacy SOPs for each system to retain access.	Partially Implemented
				12	USSS should overhaul the oversight of mandatory privacy training, to include organizational awareness for the handling and safeguarding of personally identifiable information; privacy incident handling, reporting, and mitigation practices; and compliance documentation requirements.	Partially Implemented
3	Customer Profile Management Service & National Appointment Scheduling System	USCIS	10/11/2017	5	USCIS should finalize a NARA-approved retention schedule for NASS if it has not already done so.	Partially Implemented

4	Electronic System for Travel Authorization (ESTA)	CBP	10/27/2017	3	As a best practice, the ESTA Program should consider developing and providing more clear instructions to applicants aimed at reducing the inaccurate inclusion of non-identifier information in the social media 'free-text' portion of the online application.	Not Implemented (udpate expected once collection is mandatory, see 7/29/2019 SORN)
5	Publically Available Social Media Monitoring and Situational Awareness Initiative	OPS	12/8/2017	1	OPS should fully implement DHS Instruction 047-01-008, DHS Privacy Incident Handling Guidance. 10 OPS Privacy Officer must follow up to see that there is a reasonable assurance that a NOC MMC PII spill (however rare) will ultimately be reported to DHS Enterprise Security Operations Center.	Partially Implemented
				2	OPS should fully implement DHS Instruction 047-01-005 for Component Privacy Officers11 to oversee privacy compliance, policy, and oversight activities in general and to ensure the internal NOC MMC controls keep pace with existing DHS privacy policy and best practices.	Partially Implemented
				3	As a best practice, OPS Privacy Officer should test the general incident reporting procedures for suspected or confirmed breaches as well as identify appropriate mitigations and lessons learned.	Partially Implemented
6	Privacy Incidents Affecting Individuals Protected by Section 1367	USCIS, USCG, ICE	2/4/2019	1	Components with systems containing Section 1367 information, including all Components with a criminal justice law enforcement or immigration law enforcement mission, should develop implementing instructions, SOPs, or other policy guidance to ensure compliance with the confidentiality rules under Section 1367, tailored to the specific context of their missions and systems.	Not Implemented
		USCIS		2	By September 2019, USCIS must report system access inventory findings to PRIV and CRCL, including how it has addressed gaps in 1367 confidentiality protections.	Partially Implemented
		USCIS		3	USCIS must identify an ISAA with FBI that covers bulk sharing.	Not Implemented
		CBP		4	By February 2019, CBP will report to PRIV and CRCL whether all of its system interfaces and online query responses are configured to ensure only authorized users receive 1367 records, with caveats, as appropriate.	Not Implemented

Inquiries regarding outstanding recommendations should be addressed to Shannon Ballard, Director, Privacy Overisght at shannon.ballard@hq.dhs.gov.