OFFICE OF INSPECTOR GENERAL

CBP's Office of Professional Responsibility's Privacy Policies and Practices

Homeland Security

August 29, 2016

OIG-16-123

DHS OIG Highlights

CBP's Office of Professional Responsibility's Privacy Policies and Practices

August 29, 2016

Why We Did This Inspection

In response to a request from Senator Tom Coburn, we reviewed U.S. Customs and Border Protection's (CBP) Office of Professional Responsibility's (OPR) actions to determine whether its collection, storage, and sharing of sensitive personally identifiable information (PII) violated the *Privacy Act of 1974* or Department policies. We also sought to determine whether CBP OPR's policies and training for protecting sensitive PII are adequate.

What We Recommend

We recommend that CBP revise its privacy policies to address its law enforcement priorities and require more specific privacy training for CBP OPR employees.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

While investigating two individuals who trained people on counter-measure techniques for passing polygraph exams, CBP OPR collected, enhanced, stored, and shared sensitive PII. In one investigation, after confirming the individuals had extensive contact with the subject of the investigation, CBP OPR shared the sensitive PII of up to 174 individuals with 11 Federal agencies. In the other investigation, CBP OPR shared the sensitive PII of up to 4,825 individuals multiple times with 30 agencies, although it was not clear these individuals had received in-person polygraph training. CBP OPR's own analysis of the individuals in the second investigation revealed that some may not have been Federal employees or applicants, located in the United States, or alive.

In both investigations, CBP OPR's collection, enhancement, and storage of the sensitive PII complied with the *Privacy Act of 1974* and Department of Homeland Security policies. However, although CBP OPR was allowed to share the sensitive PII with other Federal agencies, we do not believe the sharing of information with 30 agencies in the second investigation met the intent of what was allowed. Further, the manner in which the information was shared violated aspects of the *Privacy Act of 1974* and DHS policies. Specifically, CBP OPR staff did not appropriately document disclosure of the sensitive PII, password protect it, or properly restrict its further dissemination. Because of this lack of protection, each time the sensitive PII was shared its vulnerability increased. We believe the manner in which CBP OPR shared the sensitive PII showed a lack of regard for, and may have compromised these individuals' privacy. We attribute this to CBP OPR's general belief that accomplishing its law enforcement mission takes precedence over its responsibility to protect individuals' privacy.

CBP Response

CBP concurred with our recommendations and is taking steps to address them. Based on CBP's response to our draft report, we consider both recommendations resolved and open.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

August 29, 2016

MEMORANDUM FOR: The Honorable R. Gil Kerlikoswke
Commissioner
U.S. Customs and Border Protection

FROM: John Roth
Inspector General

SUBJECT: *CBP's Office of Professional Responsibility's Privacy and Policy Practices*

Attached for your information is our final report, *CBP's Office of Professional Responsibility's Privacy and Policy Practices*. We incorporated the formal comments from the Office of Professional Responsibility in the final report.

The report contains two recommendations aimed at improving CBP's operations. Your office concurred with both recommendations. Based on information provided in your response to the draft report, we consider the two recommendations resolved and open. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) corrective action plan and (2) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Anne L. Richards, Assistant Inspector General, Office of Inspections and Evaluations, at (202) 254-4100.

Attachment

Table of Contents

Appendixes

Abbreviations

CBP	U.S. Customs and Border Protection
DIA	Defense Intelligence Agency
DOB	date of birth
FBI	Federal Bureau of Investigation
OIG	Office of Inspector General
OPM	Office of Personnel Management
OPR	Office of Professional Responsibility
PDO	Privacy and Diversity Office
PII	personally identifiable information
SORN	System of Records Notice
SSN	Social Security number
USC	U.S. Code

Background

The mission of U.S. Customs and Border Protection's (CBP) Office of Professional Responsibility (OPR) is to promote the integrity and security of the CBP workforce. The office screens potential CBP employees for suitability, educates employees about their obligations regarding integrity, investigates allegations of employee misconduct, and evaluates security threats to CBP.

When conducting investigations or inspections, CBP OPR employees collect, enhance, store, and share personally identifiable information (PII). PII is "any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the United States, or employee or contractor to the Department."[1] Examples of PII include an individual's name, email address, home address, and telephone number.

DHS considers PII sensitive when the information, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some information is sensitive PII on its own, such as Social Security numbers (SSN), driver's license numbers, financial account numbers, or biometric identifiers. PII can become sensitive if paired with another identifier, such as an individual's date of birth (DOB), citizenship or immigration status, the last four digits of SSN, mother's maiden name, or criminal history.

Laws and Policies Governing the Use of PII at DHS

Federal laws and policies govern the collection, enhancement, storage, and sharing of PII held in a Federal agency's system of records. A system of records is any group of records under the control of an agency from which information is retrieved by the name of the individual or some other assigned identifier.[2] For example, DHS' Internal Affairs records may include PII of individuals undergoing background investigations as part of the job application process. The records also include PII of employees under an integrity or disciplinary inquiry investigation. CBP OPR's records are considered part of the DHS Internal Affairs' system of records.[3]

---

[1] *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information,* DHS Privacy Office, March 2012
[2] 5 U.S. Code (USC) 552a(a)(5)
[3] Federal Register, Volume 73, 67529, November 14, 2008; DHS amended the system of records as published in the Federal Register, Volume 79, 23361, April 28, 2014.

The *Privacy Act of 1974* (Privacy Act)[4] provides protections for individuals' personal information held in an agency's system of records. The Privacy Act:

- requires agencies to maintain only information about an individual that is relevant and necessary to accomplish an agency purpose required by statute or by executive order;
- forbids agencies from maintaining records describing how any individual exercises rights guaranteed by the First Amendment, unless authorized by statute or by the individual or unless relevant to an authorized law enforcement activity; and
- requires agencies to limit their sharing of individuals' records to specific reasons outlined in the Privacy Act, such as a routine use (a use compatible with the purpose for which it was collected) or for law enforcement purposes.

The Privacy Act also requires agencies to publish a System of Records Notice (SORN) in the Federal Register detailing, among other information, the categories of individuals included in the system, the types of records maintained on these individuals, and the routine uses of the information.

The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* (handbook) provides guidance to employees on protecting records containing sensitive PII and what to do if sensitive PII is compromised. According to the handbook, sharing sensitive PII outside of DHS is authorized only if the following three criteria are met:

- The recipient's need for the information is related to his or her official duties.
- A published routine use is included in the applicable SORN.
- An Information Sharing and Access Agreement or a formal request for information is in place for disclosures of the information.[5]

When emailing sensitive PII outside of DHS, according to the handbook, employees are to send the information in an encrypted attachment and provide a password separately.

---

[4] 5 USC 552a

[5] The March 4, 2003 *Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing* serves as the current Information Sharing and Access Agreement between DHS, the Intelligence Community, and any department or agency with Federal law enforcement responsibilities. Per 5 USC 552a(b)(7), DHS can also share information with another government agency for a civil or criminal law enforcement purpose, upon request from the head of the other agency.

DHS also has guidance on the use of PII gathered from commercial data. For example, DHS privacy experts recommend that because commercial data varies in quality and integrity, components should assess whether it is sufficiently reliable before using it for law enforcement purposes.

Appendix C contains more details about the laws and policies governing handling of PII at DHS.

CBP OPR Investigations

In April 2011, CBP OPR administered a polygraph examination to a CBP job applicant who later admitted to being trained by Chad Dixon on passing polygraph examinations. CBP OPR opened an investigation of Mr. Dixon in July 2011. Investigators found Mr. Dixon operated a business training customers, including two CBP applicants, on countermeasures designed to conceal disqualifying information during polygraph examinations conducted by various Federal agencies. As a result of the investigation, Mr. Dixon pleaded guilty, in part, to obstruction of an agency proceeding, in violation of 18 USC 1505, endeavoring to "influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States." In September 2013, he was sentenced to 8 months in prison followed by a 3-year term of supervised release and ordered to forfeit more than $17,000.

Subsequent to taking a pre-employment polygraph examination in May 2009, a CBP job applicant admitted to lying during the examination and to purchasing a training manual on passing polygraph examinations from Douglas Williams. CBP OPR opened an investigation of Mr. Williams in June 2012. In May 2015, Mr. Williams pleaded guilty to a five-count indictment, including charges of witness tampering and mail fraud, and training customers to lie and conceal crimes and other misconduct during polygraph examinations. In September 2015, Mr. Williams was sentenced to 2 years in prison.

Request for Office of Inspector General Review

On November 14, 2013, a McClatchy News Service online article described CBP OPR's two investigations, reporting that in one instance, the component had shared a list of 4,904 individuals with nearly 30 Federal agencies.[6] The article alleged that many individuals on the list were not Federal employees, were not seeking Federal employment or security clearances, or had limited interaction with Williams. According to the article, CBP "ended up scrutinizing people who had no direct ties to the U.S. government and simply had purchased certain books."

[6] See http://www.mcclatchydc.com/news/special-reports/insider-threats/article24758938.html, last accessed October 1, 2015.

In a March 13, 2014 letter, Senator Tom Coburn expressed his concern to the DHS Office of Inspector General (OIG) that CBP OPR had violated DHS policy, Federal regulation, and law when it shared PII during the two investigations. He alleged that individuals on the list "were not federal employees, and were not actively seeking federal employment," and that "the law enforcement purpose of keeping a record of their book purchase [was] not evident." Senator Coburn requested that DHS OIG "identify the source of every piece of information CBP OPR shared" and "identify every recipient of the information outside of DHS."

Results of Inspection

During the investigations of Mr. Dixon and Mr. Williams, CBP OPR collected, enhanced, and stored the sensitive PII appropriately. CBP OPR was permitted to share the sensitive PII with other DHS entities and Federal agencies to further its investigations, but in the Williams investigation we question whether CBP OPR's sharing of the information was truly for that purpose. Further, CBP OPR shared the information in a manner that did not comply with certain aspects of the Privacy Act and DHS policies and with little regard for individuals' privacy. We attribute this failure to properly safeguard sensitive PII to CBP OPR's belief that accomplishing its law enforcement mission takes precedence over its responsibility to protect individuals' privacy. In the past, CBP OPR has not always recognized the importance of safeguarding sensitive PII and protecting privacy. This attitude is compounded by employees' perception that some required procedures may potentially hinder investigations and that training is not specific enough for law enforcement, as well as many employees' unfamiliarity with privacy policies.

CBP OPR Collected, Enhanced, and Stored Sensitive PII According to Applicable Law and Department Policies

In both investigations, CBP OPR collected PII according to Federal law and DHS policies. CBP OPR used search warrants and other investigative techniques to obtain evidence against Mr. Dixon and Mr. Williams. During the Dixon investigation, OPR collected about 30,000 phone numbers related to potential clients from communications records, information from his schedule book, credit card receipts, and notes about clients who were trained on passing polygraphs. In the Williams investigation, CBP OPR obtained Williams' customer mailing list containing the names and addresses of 4,904 individuals who, at a minimum, purchased training materials. CBP OPR personnel said the purpose of collecting the PII was to identify a list of witnesses and possible co-defendants to further their law enforcement investigations.

The collection of PII of individuals who may have, at a minimum, only purchased a training manual on passing polygraphs complies with the Privacy Act because, under the Act, agencies can maintain information on an individual's First Amendment activities (in this case, freedom of speech and freedom of association) if within the scope of an authorized law enforcement activity. Because CBP OPR collected the PII as part of its law enforcement investigations of Mr. Dixon and Mr. Williams, the collection was permissible. The collection also complied with the DHS handbook, which requires components to have the legal authority to collect the data and a SORN describing the data. The DHS Internal Affairs SORN describes the types of individuals it covers as: "Any applicants for Federal employment, past and present employees, contractors, and contractor applicants, or any other individual who is subject to, or involved in, an integrity or disciplinary inquiry or investigation."

For both investigations, CBP OPR enhanced the PII it initially collected within the bounds of the law. OPR personnel used various data sources, including one commercial database, to further develop the initial PII. Table 1 shows the government and commercial databases CBP OPR used to enhance the PII.

Table 1: Government and Commercial Databases Used in Investigations

Data Source	Purpose	Used in Dixon investigation	Used in Williams investigation
Commercial Database			
Accurint	To gather identifying information such as names, SSNs, and addresses	X	X
Government Databases			
Passport records in Consolidated Consular Database	To verify SSNs and to identify whether individuals held official or diplomatic passports	X	X
TECS[7]	To determine whether individuals were associated with Federal law enforcement	X	X
National Crime Information Center	To obtain criminal histories	X	X
eLibrary	To identify bank information based on credit card numbers	X	
Driver's license databases	To obtain pictures of individuals	X	
CBP OPR background investigation files	To identify current or potential CBP employees	X	X

Source: OIG analysis of CBP OPR data

The purpose of enhancing the initial PII was to develop a list of potential witnesses and possible co-defendants for both investigations. In the Dixon

[7] CBP uses TECS to help vet and determine the admissibility of people arriving in the United States.

investigation, CBP OPR analyzed an initial list of about 30,000 phone numbers and narrowed it to 174 individuals who had initiated contact with Mr. Dixon and subsequently communicated with him through his personal cell phone at least 3 times. CBP OPR then enhanced the PII of these 174 individuals with information gathered from the databases described previously.[8] In the Williams investigation, CBP OPR started with an initial list of about 5,000 individuals and, after removing deceased individuals, ended up with a list of 4,825 individuals. CBP OPR then enhanced the PII of the 4,825 individuals with information from the databases.

OPR's enhancement of the initial PII was appropriate and complied with the routine uses described in the applicable SORNs. For example, according to the National Crime Information Center SORN, information from its database may be disclosed "[to] criminal justice agencies to conduct background checks." The DHS Internal Affairs SORN permits the use of records from any of the Department's internal affairs systems, including CBP's, for "investigating or prosecuting a violation … where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law." Also, using commercial data in the Accurint database to enhance the PII was appropriate; to ensure its reliability, CBP OPR supplemented the commercial data with information found in the government databases, as recommended by DHS privacy experts.

Finally, CBP OPR appropriately stored the sensitive PII. According to CBP officials, all CBP-issued laptops are fully encrypted, which complies with the handbook regarding where to store sensitive PII. CBP OPR personnel also told us they stored hard copies of their work products in locked cabinets or in sealed boxes and controlled access to the PII to those who needed it to perform their official duties, as required by the handbook.

CBP OPR's Intent in Sharing the Sensitive PII Is Questionable

Under the Privacy Act and DHS policies, CBP OPR was permitted to share individuals' sensitive PII during the investigations of Mr. Dixon and Mr. Williams to further its investigations and share information with law enforcement agencies when the information indicated a violation or potential violation of law. However, we question whether the sharing of the information with so many Federal agencies during the Williams investigation was a genuine effort to meet either purpose. Further, the way in which CBP OPR shared the sensitive PII did not comply with the Privacy Act or DHS policies, potentially compromising the individuals' privacy and showing an apparent lack of regard for their privacy.

[8] We could not fully analyze the sensitive PII of the 174 individuals because grand jury secrecy rules protected the records.

CBP OPR's Sharing of Sensitive PII in the Dixon Investigation

In the Dixon investigation, CBP OPR shared a list with sensitive PII of 174 individuals with 4 agencies, as well as smaller portions of the list with another 5 agencies. One agency, the Federal Bureau of Investigation (FBI), which originally received sensitive PII from CBP OPR, forwarded the list to the Office of Personnel Management (OPM). Figure 1 summarizes the sharing of sensitive PII in the Dixon investigation.

Figure 1: Sharing of Sensitive PII in Dixon Investigation – 10 Agencies Received Sensitive PII

During the Dixon investigation, CBP OPR shared a list of 174 individuals that included the following sensitive PII: name, DOB, SSN, phone number, address, and miscellaneous notes with:

- FBI special agents and Department of Justice prosecutors
  - FBI then forwarded the list to OPM to determine Federal employment and security clearance status
- Two Department of Defense OIG Defense Criminal Investigative Service employees
- DHS OIG investigator assisting with the investigation

CBP OPR shared smaller portions of the list with other agencies when it identified employees at the agencies or another agency within their jurisdiction:

- Drug Enforcement Administration
- Food and Drug Administration
- Naval Criminal Investigative Service
- National Security Agency
- U.S. Postal Inspection Service (CBP OPR only provided a report of investigation including sensitive PII.)

Source: OIG analysis of CBP OPR data

According to the Privacy Act, an agency may share information from its system of records if it is compatible with an applicable routine use in the SORN. The DHS Internal Affairs SORN governing CBP OPR's data permits, as a routine use, the disclosure of information "[t]o third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation." To that end, in the Dixon investigation, CBP OPR shared the sensitive PII of specific individuals with agencies where the individuals were employed to request interviews and gather additional evidence. Another routine use is the sharing of information with an appropriate law enforcement agency "charged with investigating or prosecuting a violation … where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law." Under this routine use, CBP

OPR shared the sensitive PII of 11 sex offenders it identified among Mr. Dixon's potential clients to Department of Justice prosecutors. The prosecutors then notified the individuals' parole and probation officers because these convicted sex offenders may have been required to submit to periodic polygraph examinations.

CBP OPR also complied with the DHS handbook when it shared sensitive PII. During the investigation, CBP OPR met the three requirements: it shared sensitive PII with individuals whose need for the information was related to their official duties; there was an applicable routine use in the relevant SORN; and an information sharing agreement was in place.

CBP OPR's Sharing of Sensitive PII in the Williams Investigation

In the Williams investigation, CBP OPR shared a list of 4,825 individuals that contained sensitive PII with 7 agencies and smaller portions of the list with an additional agency. OPR identified the individuals on the list through Mr. Williams' customer mailing list. They had, at a minimum, purchased his training manual; any other interaction with Mr. Williams (whether they had met in person or otherwise communicated with him) was unknown.

The sensitive PII on this list of 4,825 individuals included DOBs, SSNs, and other demographic information about the individual, including profession. The list contained 4,558 DOBs and 4,600 SSNs. Table 2 shows the top 10 professions on the list.

Table 2: Top Ten Professions from Williams' Customer Mailing List*

Profession	Number
Police Officer	132
CBP-affiliated (current or former employee or applicant for employment)	**111**
Firefighter	106
U.S. Army	62
Teacher	61
U.S. Navy	44
Registered Nurse	38
Attorney	37
Physician	28
Paramedic	24

Source: OIG analysis of CBP OPR data
* Some individuals on the list had multiple professions.

CBP OPR analysts included the professions for 1,396 individuals on the list. In total, 444 (31.8 percent) of the individuals were connected to the Federal Government, including CBP applicants or employees (former or current), military personnel, Federal law enforcement personnel, and individuals in the

Intelligence Community. The remaining 952 individuals (68.2 percent) had no apparent affiliation with the Federal Government and included diverse professions, such as an actor, biochemist, casino dealer, chiropractor, professional golfer, priest, and massage therapist. We also noted that 102 individuals on Williams' customer mailing list had mailing addresses outside of the United States, for example, in Canada, the United Kingdom, Singapore, Israel, and South Africa. In addition, even though CBP OPR personnel told us that they removed deceased individuals from the list, 64 individuals were identified as deceased.

Personnel at the Defense Intelligence Agency (DIA), who received the sensitive PII from CBP OPR, later suggested sending the data to "each agency within the U.S. Government" that had a polygraph program. CBP OPR agreed, and DIA disseminated sensitive PII to 22 Federal agencies. Figure 2 summarizes the sharing of sensitive PII in the Williams investigation.

Figure 2: Sharing of Sensitive PII in Williams Investigation – 30 Agencies Received Sensitive PII

During the Williams investigation, CBP OPR shared a list of 4,825 individuals that contained the following sensitive PII: name, address, phone number, SSN, DOB, and other demographic data, including the individual's profession, with:

- Department of Justice prosecutors
- FBI
- Polygraph managers at:
  - DIA
  - National Center for Credibility Assessment
  - Office of the Secretary of Defense, Office of the Under Secretary of Defense for Intelligence
  - Naval Criminal Investigative Service

For 9 months, CBP OPR also sent different portions of the list as email attachments to personnel at the 6 agencies listed above, as well as the Department of Defense OIG Defense Criminal Investigative Service and OPM. Information in the emails suggests the recipients received only portions of the client lists, such as potential clients who were convicted sex offenders or potential clients from a designated geographic area.

Based on a request from DIA, CBP OPR agreed that the list containing the sensitive PII should be disseminated to Federal agencies with polygraph programs. DIA shared the sensitive PII in 2 separate emails to individuals at the following 22 agencies:

- U.S. Coast Guard Investigative Service
- Transportation Security Administration
- U.S. Secret Service
- U.S. Immigration and Customs Enforcement
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Bureau of Prisons
- Central Intelligence Agency
- Drug Enforcement Administration
- Department of Energy
- Food and Drug Administration
- Internal Revenue Service
- National Geospatial-Intelligence Agency
- U.S. Postal Service OIG
- U.S. Postal Inspection Service
- Department of Veterans Affairs OIG
- CBP OPR*
- DIA*
- Department of Defense OIG Defense Criminal Investigative Service*
- Department of Justice*
- FBI*
- National Center for Credibility Assessment*
- Office of Secretary of Defense*

*Different individuals at these agencies had previously received the list with sensitive PII directly from CPB OPR. The two emails from DIA were sent to additional individuals at these agencies.

Source: OIG analysis of CBP OPR data

As in the Dixon investigation, CBP OPR's sharing of sensitive PII in the Williams investigation would have been permissible under the Privacy Act, if the information was shared under applicable routine uses in the SORN. CBP OPR officials claimed sharing the sensitive PII with external agencies furthered the investigation by helping to determine whether any individual received polygraph training from Mr. Williams. This would be a routine use under the SORN — sharing information during a law enforcement investigation to obtain "information pertinent to the investigation." CBP OPR officials also indicated they shared the information under another routine use — sharing information with law enforcement agencies when the information indicates a violation or potential violation of law — so other Federal agencies could determine whether any of their employees might have received polygraph training. The CBP OPR case agent told us that OPR did not have access to high-level databases that might have revealed links between the 4,825 individuals on the list and the Federal Government (thereby indicating a potential violation of law regarding lying on polygraph examinations), so he shared the entire list rather than attempting to narrow it down.

Further, although feedback is not required when sharing information to further a law enforcement investigation, in the Williams investigation, CBP OPR rarely received responses from agencies. This paucity of feedback, along with OPR's failure to diligently track responses, again calls into question whether OPR's sharing of sensitive PII was a genuine attempt to identify more potential witnesses or otherwise further its own investigation. In one email sharing the sensitive PII, the CBP OPR case agent demonstrated he hoped to receive information to further the investigation by writing, "Please notify me immediately if any of you discover individuals believed to have met with WILLIAMS for personal polygraph countermeasure training." However, of the 30 agencies that received sensitive PII during this investigation, CBP OPR received responses from 4 — the Department of Defense OIG Defense Criminal Investigative Service, DIA, FBI, and OPM. The OPR case agent told us he did not record whether agencies responded to him, and we could not find any other responses.

Because of the criticality of their mission, the Privacy Act gives law enforcement officials wide latitude in sharing PII. But the mission's criticality, along with the importance of maintaining public trust, also make it imperative that law enforcement officials not take advantage of their authority and fail to safeguard individuals' privacy. In the Williams investigation, we believe CBP OPR could have satisfied both routine uses by sharing more limited portions of the list, but CBP OPR appears to have overlooked its crucial responsibility by sharing the sensitive PII of more than 4,800 individuals without sufficient reason.

The Manner in Which CBP OPR Shared Sensitive PII Did Not Always Comply with the Privacy Act or DHS Policies

CBP OPR did not always document its disclosures of sensitive PII, password protect sensitive PII in electronic transmissions, or obtain consent from the agencies that originated the information to further disseminate it. OPR's failure to protect the sensitive PII by consistently taking such actions potentially compromised individuals' privacy.

First, according to the Privacy Act, Federal agencies must track the date, nature, and purpose of each disclosure of information from their records, as well as to whom the information was disclosed. CBP personnel told us that the component uses the *Privacy Act Disclosure Record* (DHS Form 191) to document disclosures. At the time of our review, CBP did not have a written policy requiring use of DHS Form 191. In the Dixon investigation, the CBP OPR investigator completed these forms in 2 of 15 instances. In the Williams investigation, CBP OPR personnel did not complete any of these forms.

CBP OPR did not formally track every time it shared the sensitive PII, so we cannot be certain we know about every instance of sharing. When we asked the CBP OPR case agent how he documented the sharing of the sensitive PII in the Williams investigation, he told us that he accounted for all instances of sharing in his report of investigation. We reviewed the draft report of investigation.[9] It describes, in part, how DIA forwarded the sensitive PII to "the Polygraph Program Managers (PM) of each agency within the U.S. Government," but the report does not further identify these agencies. We learned that DIA forwarded the sensitive PII to at least 22 agencies only after we reviewed hundreds of emails from the investigation.

Second, according to the handbook, when emailing sensitive PII outside of DHS, the sender should encrypt the information in an attachment and provide the password separately. Of the nine emails we reviewed in which CBP OPR shared PII in the Dixon investigation, seven appeared to have password-protected attachments. In the Williams investigation, CBP OPR was not as diligent at protecting the sensitive PII. Of the 31 emails with sensitive PII that CBP OPR shared in the Williams investigation and that we were able to review, only 3 appeared to have password-protected attachments. We are not aware of any incidents in which the PII was unintentionally revealed, but we are still concerned that the sensitive PII of these individuals was shared in this manner.

[9] The final report of investigation was not available at the time of our review.

Third, CBP OPR personnel told us they follow the "Third Agency Rule," meaning data contained in a CBP system of records should not be shared externally without specific approval of the agency from which the data originated. During our review of CBP OPR email communications, we observed that CBP OPR follows this rule by including disclaimer language in emails explaining that the data cannot be further disseminated or used as evidence without the originating agency's authorization. The disclaimer language reads, in part, "This information shall not be distributed beyond the original addressees without prior authorization of the originator."

In the Dixon investigation, the disclaimer language was unnecessary because Grand Jury secrecy requirements governed the disclosure of the sensitive PII. In the Williams investigation, the OPR case agent sent 31 separate emails containing sensitive PII; 24 did not include the third-party disclaimer language. We are unaware of any instances in which the sensitive PII was further disseminated, but we cannot be certain that the external agencies who received data from CBP OPR did not share the information. Again, this shows a disregard for the individuals' sensitive PII.

Ultimately, we may never be able to substantiate the full extent to which the sensitive PII was shared during the investigations, either by CBP OPR or by agencies who received the information from CBP OPR.

CBP OPR Continues to Struggle with Its Responsibility to Safeguard Sensitive PII and Protect Privacy

Because CBP has struggled to ensure proper handling of sensitive PII and safeguarding of individuals' privacy, in August 2014, the component issued procedures designed to better protect privacy. CBP OPR personnel expressed concern that the August 2014 procedures could hinder their investigations; they also believe current privacy guidance and training are not specific enough for the law enforcement mission. Finally, many CBP OPR employees are unfamiliar with some aspects of privacy policies.

CBP OPR Has Had Difficulty Protecting Individuals' Privacy

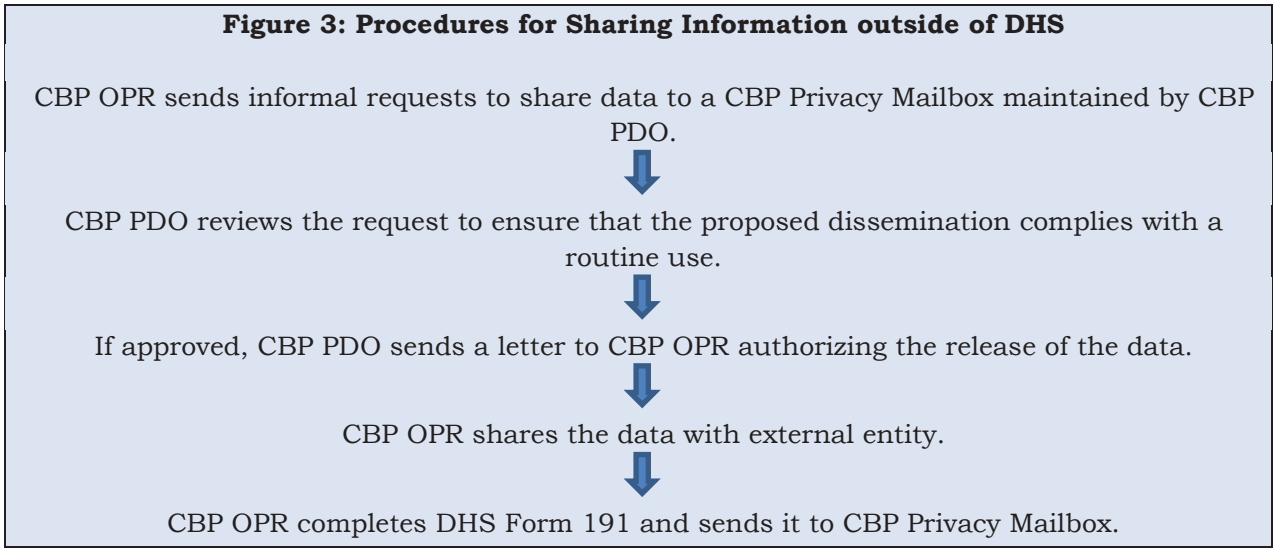
In an April 2012 review of CBP's privacy stewardship, OIG concluded, "CBP had made limited progress toward instilling a culture of privacy that protects sensitive PII … in part because it has not established a strong organizational approach to address privacy issues across the component." As a result of the review, CBP issued a directive intended to hold CBP leaders accountable for their employees' understanding of and compliance with their privacy responsibilities and implemented measures intended to protect employees' SSNs.

In 2011, during a joint pilot designed to improve CBP's background investigation process, CBP OPR shared the sensitive PII of about 3,000 CBP employees with the FBI. After investigating whether the sharing was appropriate, the DHS Privacy Officer released an Information Memorandum in July 2012 noting that "CBP IA [OPR] demonstrated poor stewardship of employee PII during the [pilot]." Further, according to the memorandum, CBP OPR leadership "disregarded privacy concerns raised repeatedly about the [pilot]," and there was a "lack of oversight by CBP IA [OPR] leadership to ensure that DHS policies governing the sharing of PII were adhered to." The DHS Privacy Officer wrote that she had "serious concerns about how the [pilot] was conducted and specifically about the attitude of CBP IA [OPR] leadership … toward the privacy considerations that should have been addressed."

CBP Attempted to Improve Guidance for Protecting Sensitive PII

In response to the July 2012 Information Memorandum, CBP's Privacy and Diversity Office (PDO) and OPR developed and, in August 2014, issued standard operating procedures for information sharing, which addressed previously lacking areas. Figure 3 contains information from the procedures on sharing information.

Figure 3: Procedures for Sharing Information outside of DHS



Source: CBP

According to the procedures, if "… an immediate release authorization is necessary in order to respond to an emergency situation, OPR will contact the CBP Privacy OPR Liaison to request expedited review and authorization." Also according to the procedures, CBP OPR should ensure that partners who receive information only use it for specified purposes and do not share the information further with third parties without CBP OPR's express permission.

In January 2015, CBP issued a component-wide privacy directive establishing procedures for collecting, using, and safeguarding PII.[10] The directive reiterates that the DHS Form 191 must be prepared every time information is shared from a CBP system of records, and a copy must be submitted to the CBP Privacy Mailbox. The directive also clarifies the responsibilities of the Privacy Liaison position as the point of contact and "initial identifier of privacy issues" on behalf of each CBP office.

CBP OPR Continues to Have Problems Safeguarding Privacy

CBP privacy officials described the ongoing challenge to protect PII and, at the same time, ensure that CBP, the largest law enforcement organization in the United States, accomplishes its national security mission. One official explained that the component has access to large amounts of PII, but needs a balanced approach to sharing. The privacy official said that in a law enforcement agency, protecting PII may appear to conflict with national security interests, but the component must ensure it is not perceived as abusing its access to information. Another senior DHS privacy official echoed the struggle, telling us that any hesitation to share information should be weighed against criticisms levied against law enforcement after September 11, 2001, namely that there was not enough information sharing.

This internal conflict was evident when CBP OPR first tried to implement the procedures for information sharing: when presented to CBP's Assistant Commissioner for OPR in December 2013, he refused to sign them. The procedures were implemented in August 2014, 8 months later, when a new Assistant Commissioner signed them. In her July 2012 Information Memorandum, the DHS Privacy Officer also noted that the Assistant Commissioner appeared to believe CBP OPR's mission exempted it from privacy laws and DHS privacy policies.

In interviews, CBP OPR personnel in field offices expressed concern that following the August 2014 procedures could delay investigations and hamper the law enforcement mission. Several employees told us the information sharing process in the procedures could hold up investigations because approving officials might not process requests promptly or be available to approve them when necessary. For example, one CBP OPR manager told us that, at the time of our interview, he had been waiting 3 weeks for a response from CBP PDO about whether data could be shared. An official from CBP PDO confirmed that delays were likely, attributing them to staffing shortages. Several employees also said the process could affect CBP OPR's relationships with law enforcement partners.

[10] CBP Directive No. 2120-010, *Privacy Policy, Compliance, and Implementation*, January 2, 2015

CBP OPR personnel said they believe privacy training is ineffective because it is not geared toward an investigative entity with law enforcement responsibilities. Fifty of 96 (52 percent) of interviewees said their privacy training was not specific enough for the law enforcement environment.

CBP OPR Staff Are Not Familiar with Existing Privacy Policies

Finally, our interviews with CBP OPR staff revealed a lack of knowledge and understanding of existing privacy guidelines and policy. The majority of CBP OPR staff collected and shared sensitive PII, either internally within DHS or externally, as part of their job responsibilities. However, when we asked staff to define sensitive PII, 63 of 96 (66 percent) could not properly define the term. Their definitions incorrectly identified sensitive PII as related to:

- individuals in high-profile positions;
- confidential informants; and
- national security information.

Slightly more than half (50 of 96 interviewees) thought there was no difference between PII and sensitive PII. When we asked whether they knew their sharing of PII was covered under a routine use from a system of records, 72 percent (69 of 96) responded they did not know. Only four individuals indicated sharing for law enforcement purposes as a routine use.

In its liberal sharing and loss of control over the sensitive PII of nearly 5,000 people, CBP OPR did not properly protect sensitive PII. Better guidance and training should help CBP OPR understand its responsibilities, but CBP OPR must also accept its responsibility to minimize the risk to individuals' privacy. This will require understanding the potential damage, as well as consistently applying the protections already in place.

Recommendations

We recommend that CBP:

Recommendation 1: Revise the CBP OPR standard operating procedures for information sharing to address its law enforcement priorities and to comply with all aspects of the CBP Privacy Directive.

Recommendation 2: Require more specific training on Federal, departmental, and CBP privacy policies and guidelines for CBP OPR personnel.

OIG Analysis of CBP Management Comments

CBP concurred with our recommendations and is taking steps to address them. Appendix B contains a copy of CBP's management comments in their entirety. We also received and incorporated technical comments as appropriate. We consider Recommendations 1 and 2 to be resolved and open. A summary of CBP's responses and our analysis follows.

CBP Response to Recommendation 1: CBP concurred with the recommendation. According to CBP, PDO will collaborate with CBP OPR to revise the standard operating procedures for information sharing to comply with all aspects of DHS and CBP Privacy Directives while addressing CBP OPR's law enforcement priorities. CBP estimated this would be completed by December 31, 2016.

OIG Analysis: CBP's planned action is responsive to the recommendation. We consider the recommendation resolved and open. We will close this recommendation upon receipt of the revised standard operating procedures.

CBP Response to Recommendation 2: CBP concurred with the recommendation. According to CBP, PDO will coordinate with CBP OPR to develop and deliver a formal training program to help OPR personnel understand how privacy and properly handling of sensitive PII interplay in their day-to-day work. CBP estimated this would be completed by December 31, 2016.

OIG Analysis: CBP's planned action is responsive to the recommendation. We consider the recommendation resolved and open. We will close this recommendation upon review of the formal training program.

Appendix A
Objectives, Scope, and Methodology

DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

On November 14, 2013, the McClatchy News Service published an article alleging that CBP OPR distributed a list of 4,904 people and their PII to nearly 30 Federal agencies. On March 13, 2014, Senator Coburn requested that DHS OIG determine the source of every piece of information CBP OPR shared in these incidents, identify every recipient of the information outside of DHS, and determine whether CBP OPR violated the Privacy Act, DHS policies, or Federal law.

Our objectives were to determine whether:

- CBP OPR appropriately collected, stored, and shared PII in this incident;
- CBP OPR's policies and agreements regarding PII are adequate; and
- CBP OPR's privacy practices for sharing PII information comply with law and DHS policies.

We conducted our fieldwork between June 2014 and June 2015. We interviewed CBP and DHS officials with knowledge of the investigations and information sharing incidents and DHS officials who previously reviewed information sharing practices within CBP OPR. We also interviewed CBP OPR employees in six field offices—Washington, DC; New York, New York; Newark, New Jersey; Houston, Texas; Los Angeles, California; and Tucson, Arizona. At the field offices, we interviewed 96 CBP OPR field employees regarding their understanding of PII sharing policies and practices. Finally, we reviewed information sharing policies, directives, and handbooks; Federal regulations; and laws.

CBP OPR's investigations included grand jury material. Further, during our fieldwork, CBP OPR's investigation of Mr. Williams was open. We discuss details of the investigations affected by these factors only to the extent necessary to meet our objectives.

We conducted this review under the authority of the *Inspector General Act of 1978*, as amended, and according to the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency. We identified a possible appearance of impairment to our organizational independence. Our Office of Investigations requested and served subpoenas and search warrants for CBP OPR, which produced information that may have been included in the client lists. CBP OPR shared one client list

containing PII with our Office of Investigations. This possible appearance of impairment did not affect our ability to perform this inspection, as well as report our findings and conclusions impartially.

Appendix B
CBP Comments to the Draft Report

1300 Pennsylvania Avenue NW

U.S. Customs and Border Protection

MEMORANDUM FOR: Anne L. Richards
Assistant Inspector General
Inspections and Evaluations

AUG 10 2016

FROM: Sean M. Mildrew
Chief Accountability Officer
Office of Accountability

SUBJECT: Management Response to OIG Draft Report, "CBP's Office of Internal Affairs' Privacy Policies and Practices" (Project No. 14-121-ISP-CBP)

Thank you for the opportunity to review and comment on this draft report. U.S. Customs and Border Protection (CBP) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

Following 9/11, protecting the country from ever-evolving threats requires agencies like CBP to share information across traditional organizational boundaries. CBP's Office of Professional Responsibility (OPR) opened criminal investigations on two subjects who profited from, and were eventually convicted of, training thousands of individuals, including job applicants for CBP law enforcement positions, on how to lie and conceal criminal behavior and other misconduct during pre-employment polygraph examinations. CBP OPR shared information gleaned from the investigations with other federal agencies so those agencies could determine whether any of their employees might have received polygraph countermeasure training. CBP echoes the words of Assistant Attorney General Leslie R. Caldwell of the U.S. Department of Justice Criminal Division when she spoke about this specific case, "Lying, deception and fraud cannot be allowed to influence the hiring of national security and law enforcement officials, particularly when it might affect the security of our borders."

We contend that any failure on CBP's part to document the disclosures, password protect electronic transmissions, or include appropriate disclaimer language in its messaging was more attributable to procedural error than institutional indifference.

Since the conclusion of the inspection, CBP has taken affirmative measures to promote Personally Identifiable Information (PII) accountability within OPR. Most notably, we have increased the frequency of training and the types of forums and venues that address

PII information handling. In addition, CBP has appointed new senior leadership in OPR in the Assistant Commissioner and Deputy Assistant Commissioner positions who oversee all aspects of the office's operations, policies and practices. The new leadership team is keenly aware that OPR's efforts to promote the integrity and security of the CBP workforce must be accomplished in accordance with all applicable laws and policies, including those designed to protect individuals' privacy and civil rights.

The draft report contained two recommendations, with which CBP concurs. Please see the attached for our detailed response to each recommendation. Technical comments were provided under separate cover.

Again, thank you for the opportunity to comment on this draft report. If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Kimberly Dockery, CBP Audit Liaison, at (202) 325-7712.

Attachment: Department of Homeland Security (DHS) Management Response to Recommendations Contained in OIG-14-121-ISP-CBP

The Office of Inspector General (OIG) recommended that the Commissioner of U.S. Customs and Border Protection (CBP):

Recommendation 1: Revise the CBP IA standard operating procedure for information sharing to address its law enforcement priorities and to comply with all aspects of the CBP Privacy Directive.

CBP Response: Concur. CBP Privacy and Diversity Office (PDO) will collaborate with CBP OPR to revise the standard operating procedure for information sharing to comply with all aspects of the DHS and CBP Privacy Directives while addressing CBP OPR's law enforcement priorities.

Estimated Completion Date: December 31, 2016

Recommendation 2: Require more specific training on Federal, departmental, and CBP privacy policies and guidelines for CBP IA personnel.

CBP Response: Concur. CBP PDO will coordinate with CBP OPR to develop and deliver a formal training program that is in-person and webinar based, and provides real-life examples to assist CBP OPR personnel in understanding how privacy, and properly handling Personally Identifiable Information (PII) and Sensitive PII, interplays in their day-to-day work.

Estimated Completion Date: December 31, 2016

Appendix C
Laws and Policies Governing the Handling of PII at DHS

Privacy Act of 1974

The Privacy Act governs the collection, use, and dissemination of information about individuals that is maintained in systems of records by Federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

The Privacy Act requires agencies to give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records without the written consent of the individual, unless the disclosure is pursuant to 1 of 12 statutory exceptions. The Privacy Act also describes how individuals can seek access to and amend their records and sets forth various agency record-keeping requirements.

DHS Internal Affairs System of Records Notice (November 2008)

The DHS Internal Affairs system of records collects and maintains "records on applicants, past and present employees, contractors, and contractor applicants relating to integrity or disciplinary inquiries or investigations conducted by DHS Headquarters or its components, except for those investigations conducted by OIG." In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records of information contained in the DHS Internal Affairs system of records may be disclosed outside of DHS as a routine use. Of the routine uses included in the DHS Internal Affairs SORN, two are applicable to the disclosure of sensitive PII during the CBP OPR investigations of Mr. Williams and Mr. Dixon:

> **Routine Use G:** 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 and such disclosure is proper and consistent with the official duties of the person making the disclosure.
>
> **Routine Use J:** To third parties during the course of a law enforcement investigation to the extent necessary to obtain

information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

DHS Handbook for Safeguarding Sensitive Personally Identifiable Information (March 2012)

The DHS handbook applies to every DHS employee, contractor, detailee, intern, and consultant. It provides guidelines to help DHS employees safeguard sensitive PII in both paper and electronic form at DHS and provides step-by-step guidance on how to identify and protect sensitive PII. The handbook also provides instructions on encrypting, securing, and disposing of sensitive PII.

Appendix D
Office of Inspections and Evaluations Major Contributors to This Report

William McCarron, Chief Inspector
Erika Lang, Lead Inspector
Kimberley Lake de Pulla, Senior Inspector
Lindsay K. Clarke, Inspector
Renita Hunter-Caracciolo, Inspector
Glenn L. Stewart, Inspector
Kelly Herberger, Communications Analyst

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
CBP Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305