Privacy Compliance Review
of the
Office of the Chief Human Capital Officer

September 30, 2015

Contact Point
Catherine Emerson
Chief Human Capital Officer
Office of the Chief Human Capital Officer
(202) 357-8151

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Privacy Office
(202) 343-1717

I. Background

The Department of Homeland Security (DHS) Office of the Chief Human Capital Officer (OCHCO) is responsible for administering human resources services for DHS Headquarters and Components. In response to privacy incidents at OCHCO, the Chief Privacy Officer (CPO) submitted an action memo[1] on March 27, 2014 to the DHS Chief Human Capital Officer (2014 Memo) with 12 recommendations to strengthen the culture of privacy within the office. Human resources information is inherently privacy sensitive; thus, the DHS Privacy Office expects greater privacy awareness among OCHCO staff because they work with this information. Implementation of the 2014 recommendations should not be seen as a one-off exercise, but as a means to change the culture within OCHCO to meet both human resources and privacy best practices. In April 2015, the CPO initiated a Privacy Compliance Review (PCR) of OCHCO's implementation of the 12 recommendations and compliance with foundational principles for privacy policy and implementation at DHS.[2]

A PCR is designed to be a proactive and collaborative mechanism to improve a program's ability to effectuate a culture of privacy within the Department and to comply with assurances made in existing privacy compliance and other documents. An independent internal review supports decision making and performance tracking, leads to improved accountability, increases ethical and professional practices, supports effective risk management, and improves quality of output.

Between April 2015 and July 2015, OCHCO provided DHS Privacy Office staff with documents and demonstrations on OCHCO policies and procedures. OCHCO staff, particularly Gregg Pelowski, Executive Director, Human Capital Business Systems, deserve recognition for their diligent work with the DHS Privacy Office during its review and for producing all documents and information requested. Additionally, the DHS Privacy Office commends OCHCO for drafting a Privacy Action Plan, a Privacy Communication Plan, and Standard Operating Procedures and encourages the full application and sustained implementation of these plans.

During the course of this PCR, the DHS Privacy Office found that some concerns raised in the 2014 Memo remain and several recommendations from the 2014 Memo have yet to be fully implemented. As a result, the DHS Privacy Office makes an additional 25 recommendations, which mostly align with OCHCO's new Privacy Action Plan, Privacy Communication Plan, and Standard Operating Procedures.

II. Scope and Methodology

The DHS Privacy Office conducted a PCR of OCHCO's implementation of the 12 recommendations from the 2014 Memo and compliance with DHS Privacy Policy Memo 2008-01 in coordination with OCHCO leadership for the period of March 2014 through July 2015. To assess OCHCO's implementation of the CPO's 2014 recommendations and overall compliance with Privacy Policy Memo 2008-01, the DHS Privacy Office:

---

[1] See Appendix.
[2] Privacy Policy Guidance Memorandum Number: 2008-01

- Conducted site visits and received briefings and demonstrations from OCHCO division managers and staff in May, June, and August 2015;
- Developed and administered a questionnaire for OCHCO in April 2015 that included questions about:
  - Visitors/new hires
  - Document management including records retention
  - Transferring sensitive personally identifiable information (PII)
  - Document destruction
  - Data integrity
  - Unauthorized use of PII and sensitive PII
  - Information sharing
  - Training
  - Leadership
  - Overall compliance with the Fair Information Practice Principles
- Reviewed all responses to the questionnaire and provided follow-up questions to OCHCO in June 2015; and
- Reviewed all draft and final privacy related documents developed by the OCHCO Privacy Working Group.

III. 2015 Summary of Findings and Recommendations

The DHS Privacy Office makes the following 25 recommendations to improve the culture of privacy at OCHCO. The recommendations focus on the areas of transparency/raising awareness, data minimization/retention limits, use limitations, data integrity, data security, and accountability.

A. Transparency

1. Finalize and implement the OCHCO Privacy Action Plan.
2. Require that all contractors complete and submit completion certificates from DHS sponsored privacy training (which can be accessed by outside contractors via https://edit.dhs.gov/dhs-security-and-training-requirements-contractors; see "Privacy at DHS: Protecting Personal Information").
3. If still using the Contractor's Training Record form, update the form to reflect DHS Information Technology Security Awareness Training and Privacy Training links and completion certificate verification. If not using this form, verify that all contractors complete required DHS training within 30 days of assignment.

B. Data Minimization

1. Encourage Component HR offices to remove, as appropriate, SSN and date of birth from all HR related forms.
2. Complete or update PTAs for all identified systems as appropriate. The DHS Privacy Office should promptly review and mitigate all PTAs.
3. Develop and implement an OCHCO Records Management Plan.
4. Develop a means to audit compliance with existing records management processes while the OCHCO Records Management Plan is being developed. Once finalized, conduct at

least annual audits to confirm records deletion in accordance with the OCHCO Records Management Plan.
5. Implement semiannual "record clean up" days to encourage employees to delete hard copy and electronic records as appropriate.
6. Finalize guidance for records retention procedures for political appointees and career SES employees.

C. Use Limitation

1. Due to high staff turnover rates, OCHCO should regularly cross reference restricted folder permissions with current employee roster to confirm the need to retain access to folder(s).
2. Require the use of Lockbox across OCHCO, as appropriate, for those teams needing to share PII with their customers.
3. Track the number of privacy incidents caused by missing the 90-day Lockbox deletion deadline and by whom. Subsequently increase privacy and Lockbox use training as appropriate for the individual(s) and team(s).
4. Conduct at least annual audits of Lockbox to confirm data deletion requirements have been met within the 90-day time limit.

D. Data Quality and Integrity

1. Fully implement and make repeatable the tactical plan of the OCHCO Privacy Communication Plan. This could also include training on the protection of PII or sensitive PII in other HR-related training offerings.
2. Develop an enforceable means to address OCHCO employees and contractors that are more than two months overdue for required privacy training.

E. Security

1. Circulate, promote, implement, and keep current the OCHCO Privacy Standard Operating Procedures.
2. Require a PII and sensitive PII email disclaimer in all OCHCO email correspondence.
3. Track the number of Lockbox waivers requested and issued and the reasons for the waiver.
4. In conjunction with the OCHCO Privacy Communication Plan and in addition to annual privacy training, deliver team specific privacy training that focuses on areas of particular relevance to individual OCHCO teams. The DHS Privacy Office can assist in providing additional training as needed.
5. In coordination with the Office of the Chief Security Officer, provide ongoing training regarding the proper destruction of sensitive documents.

F. Accountability and Auditing

1. Reaffirm that the DCHCO is the Privacy Point of Contact and appoint an alternate Privacy Point of Contact. Include measurable goals to foster a culture of privacy within OCHCO in their performance plans.
2. Submit quarterly privacy overview reports to the DHS Privacy Office and OCHCO senior leadership to assess OCHCO implementation of the OCHCO Privacy Action Plan and any follow up actions that are formalized in the Plan.

3. Assign data steward responsibilities with appropriate authority for all OCHCO teams as appropriate.
4. Include an element in data stewards' performance plans that includes oversight of their team's use of PII and sensitive PII.
5. Include an element in direct reporting managers' performance plans that requires oversight of staff compliance with Privacy Standard Operating Procedures.

IV. Findings and Recommendations

The Privacy Office reiterates its findings and recommendations contained in the 2014 Memo and notes the status of implementation thereof. Privacy Policy Memo 2008-01 utilizes the Fair Information Practice Principles (FIPPs) to memorialize the foundational principles for privacy policy and implementation at DHS. The FIPPs provide the basis of all privacy policy development and implementation at the Department and must be considered whenever a DHS activity raises privacy concerns. During the course of this PCR, the DHS Privacy Office assessed OCHCO's implementation of the 2014 recommendations and of the FIPPs.

A. Transparency

DHS aims to create a "culture of privacy" to ensure that privacy protections are firmly embedded into the lifecycle of homeland security programs and systems. Due to the high volume of PII involved in human resources activities and due to high OCHCO staff turnover, OCHCO can improve its privacy culture by increasing the frequency of its notices to employees on the proper use and maintenance of PII. OCHCO recently finalized a Privacy Action Plan, which could significantly improve employee awareness of the responsibility to protect and properly use PII. This Plan designates concrete action(s), the team(s) responsible for implementing the action(s), and due dates. The DHS Privacy Office commends OCHCO for developing this Plan and encourages its full and ongoing implementation.

In addition to federal staff, OCHCO employs a number of on-site, off-site, part-time, and full-time contractors. These contractors are currently required to complete non-DHS hosted privacy and security training within 30 days of assignment. The DHS Privacy Office recommends that these contractors take DHS hosted privacy training to ensure that all DHS privacy policy and best practices are conveyed to the contractors in a timely fashion. OCHCO should collect completion certificates from all contractors and track training compliance for the life of the contract.

<u>Recommendations</u>

1. Finalize and implement the OCHCO Privacy Action Plan.
2. Require that all contractors complete and submit completion certificates from DHS sponsored privacy training (which can be accessed by outside contractors via https://edit.dhs.gov/dhs-security-and-training-requirements-contractors; see "Privacy at DHS: Protecting Personal Information").
3. If still using the Contractor's Training Record form, update the form to reflect DHS Information Technology Security Awareness Training and Privacy Training links and

completion certificate verification. If not using this form, verify that all contractors complete required DHS training within 30 days of assignment.

B. Data Minimization

OCHCO has taken steps to minimize the collection of sensitive PII and to collect only the 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). For example, the electronic version of training form SF-182 has been updated to prevent inclusion of Social Security number (SSN) and date of birth. OCHCO reviews security and privacy control implementation to ensure that data captured, collected and stored is minimal, and that OCHCO destroys the data in accordance with the relevant records retention schedule.

OCHCO keeps adequate track of the systems in its inventory by maintaining a "Privacy-at-a-Glance" matrix. This matrix identifies the program and the responsible team/staff, the Privacy Threshold Analysis (PTA) approval date, and whether a Privacy Impact Assessment and/or System of Records Notice is required.

The DHS Privacy Office reiterates the records retention recommendations from the 2014 Memo. Although there is a records management process in place between OCHCO and the CIO Records Management Office, it is difficult to assess compliance with records retention requirements given that OCHCO's records are subject to varying records retention periods. OCHCO is developing a Records Management Plan to provide for OCHCO-wide records disposal and has developed draft guidance for political appointees and career SES employees on removing documents when they depart the agency.

<u>Recommendations</u>

1. Encourage Component HR offices to remove, as appropriate, SSN and date of birth from all HR related forms.
2. Complete or update PTAs for all identified systems as appropriate. The DHS Privacy Office should promptly review and mitigate all PTAs.
3. Develop and implement an OCHCO Records Management Plan.
4. Develop a means to audit compliance with existing records management processes while the OCHCO Records Management Plan is being developed. Once finalized, conduct at least annual audits to confirm records deletion in accordance with the OCHCO Records Management Plan.
5. Implement semiannual "record clean up" days to encourage employees to delete hard copy and electronic records as appropriate.
6. Finalize guidance for records retention procedures for political appointees and career SES employees.

C. Use Limitation

OCHCO demonstrated that it uses PII only for authorized purposes and shares PII within and outside the Department for the purpose for which the PII was collected. OCHCO confirms those

requesting access to restricted folders have a valid need-to-know and monitors permissions on an ongoing basis.

In response to the 2014 Memo, OCHCO put in place a number of physical and procedural steps during new employee orientation and generally throughout OCHCO office space to prevent viewing of PII by individuals without a need-to-know. For example, Human Resource (HR) Specialists work in pairs during orientation so that one HR Specialist retains positive control over PII documents until they are returned to the employee. In accordance with the new OCHCO Privacy Standard Operating Procedures (SOP), floor and room access control is in place and prominently displayed signs note office space that is off limits to non-OCHCO staff. Documents containing PII are secured in a locked office, desk drawer, or file cabinet. OCHCO staff may not store PII on computer hard drives with the exception of one OCHCO team, which has the appropriate authority and equipment to do so.

Lockbox

OCHCO has taken additional steps to implement the 2014 CPO recommendations to protect PII stored on OCHCO shared drives. OCHCO's use of Lockbox[3] provides for a means to store and share privacy sensitive reports and documents between OCHCO and its customers. When OCHCO receives a request for reports that contain PII or sensitive PII, the requestor receives an email with the necessary information to retrieve the reports from Lockbox. The requestor acknowledges the file contains sensitive PII, acknowledges the need to protect the data, and confirms understanding that the file must be destroyed within 90 days. If the requestor does not confirm destruction within 90 days, a subsequent email is sent to the OCHCO Privacy Point of Contact and the lack of attestation of data deletion is considered a privacy incident.

Recommendations

1. Due to high staff turnover rates, OCHCO should regularly cross reference restricted folder permissions with current employee roster to confirm the need to retain access to folder(s).
2. Require the use of Lockbox across OCHCO, as appropriate, for those teams needing to share PII with their customers.
3. Track the number of privacy incidents caused by missing the 90-day Lockbox deletion deadline and by whom. Subsequently increase privacy and Lockbox use training as appropriate for the individual(s) and team(s).
4. Conduct at least annual audits of Lockbox to confirm data deletion requirements have been met within the 90-day time limit.

D. Data Quality and Integrity

OCHCO works to ensure that PII is accurate, relevant, timely, and complete. For example, as recommended in the 2014 Memo, one OCHCO team established a "buddy system" wherein HR Specialists verify the accuracy of key strokes after data entry by reviewing the data entry of

[3] Lockbox is a SharePoint team site with the appropriate sensitive PII labeling that uses restricted folders designated with Component name. All files within the folders are password protected.

another Specialist's personnel action input and cross referencing specific fields on hard copy documents. Another OCHCO team backs up and reviews reports of other team members before distribution.

Training

All new OCHCO employees, like all other DHS employees, are required to take privacy training as part of the on-boarding process. To increase awareness of privacy responsibilities on an ongoing basis and to implement recommendations from the 2014 Memo, OCHCO developed a Privacy Communication Plan to implement its privacy awareness campaign and provide more timely information via numerous venues. This Plan aims to foster and strengthen a culture of privacy awareness and engagement within OCHCO.

During on-the-job training sessions, HR Specialists with data entry responsibilities are reminded of the importance of accuracy of information by tenured HR Specialists who go through data entry processes and procedures. During this on-the-job training session, the importance of accurate entry is stressed as are the ramifications for inaccurate input.

Recommendations

1. Fully implement and make repeatable the tactical plan of the OCHCO Privacy Communication Plan. This could also include training on the protection of PII or sensitive PII in other HR-related training offerings.
2. Develop an enforceable means to address OCHCO employees and contractors that are more than two months overdue for required privacy training.

E. Security

OCHCO demonstrated steps taken to protect PII (in all media) against loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

New Employee Orientation

During new employee orientation for example, there is a privacy risk that PII and sensitive PII may be viewed by visitors or new hires without a need-to-know. To mitigate this risk, OCHCO HR Specialists work in pairs to better oversee new employees as they complete required HR paperwork at orientation. When needed, the HR Specialists collect all new employee personal identification documents directly from the individuals, separate the contents at a station in the back of the room away from new employees and enter or validate necessary data from the corresponding identification. All PII and sensitive PII documents are maintained under the Specialists' control at all time. Once the task is completed, all new employee identification documents are immediately returned to the corresponding new employee.

When PII or sensitive PII needs to be transferred from the new employee orientation room to OCHCO workstations, Specialists first conceal the document with PII using a Privacy Data cover sheet and then place the cover sheet and document in an opaque envelope or folder for transfer. Specialists complete data entry and once imported, paper documents are shredded, as

recommended in the 2014 Memo. When not being processed, all PII and sensitive PII are secured via locked desk, office, safe, cabinet, or drawer. In addition, easily readable signs cordon off and thus restrict access to work areas where the performance of routine work that often includes PII or sensitive PII occurs.

OCHCO Workstations

OCHCO uses PIV card readers to control access to all points of entry to the OCHCO workspace to prevent the general public from entering without authorization. Visitors cannot access certain floors from the lobby elevator without being escorted by OCHCO personnel. OCHCO has an official reception area entrance on its main office floor for visitors to sign in when meeting OCHCO personnel. All visitors are escorted and there are signs posted in areas where individuals should not enter if they do not have a business reason to be there.

In OCHCO work areas, PII and sensitive PII documents are secured in a locked office, desk drawer, or file cabinet. OCHCO staff may not store PII on computer hard drives, except for one team that has the appropriate authority and equipment to do so. OCHCO-wide, PII and sensitive PII may only be electronically stored on access restricted areas of DHS network drives and OCHCO SharePoint team sites.

In response to the 2014 Memo, OCHCO created Privacy Standard Operating Procedures to establish the responsibilities and procedures for handling PII and sensitive PII and memorialized the privacy roles and responsibilities for OCHCO managers and staff. For example, the Procedures address unattended computers, intra-office and telephone conversations, and unattended documents containing PII or sensitive PII within the office. With limited exceptions, all electronic documents containing PII or sensitive PII transferred among OCHCO offices are password protected or encrypted. Most OCHCO email correspondence includes a standard disclaimer statement that highlights the importance of PII and sensitive PII document management. The Privacy Standard Operating Procedures also require that ad hoc reports[4] that contain sensitive PII and are emailed within DHS but outside of OCHCO be disseminated by using the OCHCO Lockbox, unless a waiver is authorized. Reports that contain sensitive PII and that are emailed outside of DHS are encrypted and password protected.

Management Responsibilities

According to the OCHCO Privacy Standard Operating Procedures, OCHCO supervisors are given specific roles and responsibilities to ensure staff are made aware of these procedures and comply with them. Supervisors oversee staff and contractor privacy related training requirements. When employees telework, supervisors are responsible for communicating and ensuring that employees adhere to all applicable security, Privacy Act, and Federal Records Act provisions as well as DHS information security policies and procedures to protect government records from unauthorized disclosure, damage, or destruction.

[4] Reoccurring reports are mostly transmitted on a system to system basis.

Recommendations

1. Circulate, promote, implement, and keep current the OCHCO Privacy Standard Operating Procedures.
2. Require a PII and sensitive PII email disclaimer in all OCHCO email correspondence.
3. Track the number of Lockbox waivers requested and issued and the reasons for the waiver.
4. In conjunction with the OCHCO Privacy Communication Plan and in addition to annual privacy training, deliver team specific privacy training that focuses on areas of particular relevance to individual OCHCO teams. The DHS Privacy Office can assist in providing additional training as needed.
5. In coordination with the Office of the Chief Security Officer, provide ongoing training regarding the proper destruction of sensitive documents.

F. Accountability and Auditing

OCHCO should be accountable for complying with the FIPPs, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

In response to the 2014 Memo and due to the significant amount of PII collected and used by OCHCO, the Deputy CHCO was appointed OCHCO's Privacy Point of Contact, which is an appropriate responsibility for the DCHCO. It is equally important that an alternate Privacy Point of Contact be appointed with sufficient oversight authority and be held accountable for OCHCO's stewardship of PII. Additionally, OCHCO direct reporting managers should be held accountable for their team's compliance with OCHCO Privacy Standard Operating Procedures.

Recently, OCHCO created the role of "data stewards" who will serve as subject matter experts for their team's data and its uses and who will have key oversight for information sharing, including ensuring compliance with data destruction requirements and overall management of PII and sensitive PII. As noted in the 2014 Memo and addressed in the OCHCO Privacy SOPs, the data stewards role should also include ensuring that all PII shared by OCHCO is used for a purpose consistent with published Office of Personnel Management System of Records Notices.

Recommendations

1. Reaffirm that the DCHCO is the Privacy Point of Contact and appoint an alternate Privacy Point of Contact. Include measurable goals to foster a culture of privacy within OCHCO in their performance plans.
2. Submit quarterly privacy overview reports to the DHS Privacy Office and OCHCO senior leadership to assess OCHCO implementation of the OCHCO Privacy Action Plan and any follow up actions that are formalized in the Plan.
3. Assign data steward responsibilities with appropriate authority for all OCHCO teams as appropriate.
4. Include an element in data stewards' performance plans that includes oversight of their team's use of PII and sensitive PII.
5. Include an element in direct reporting managers' performance plans that requires oversight of staff compliance with Privacy Standard Operating Procedures.

V. Conclusion

The DHS Privacy Office appreciates OCHCO's collaborative effort in conducting this PCR and notes steps taken to implement recommendations from the 2014 Memo and to improve its ability to comply with the department's overarching privacy policies and best practices. The DHS Privacy Office will continue to support OCHCO as it undertakes to implement the 25 recommendations presented here. A self-audit is requested within six months of the date of this report and semiannually thereafter, with a written report of OCHCO findings and recommendations provided to the Chief Privacy Officer. Depending on the outcome of these self-audits, the DHS Privacy Office will determine when a future Privacy Compliance Review will occur.

VI. Privacy Compliance Review Approval

Responsible Official

Catherine Emerson
Chief Human Capital Officer
Office of the Chief Human Capital Officer

Approving Official

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Appendix

March 27, 2014 memo from DHS Chief Privacy Officer Karen Neuman to Chief Human Capital Officer Catherine Emerson

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Homeland Security

March 27, 2014

MEMORANDUM FOR: Catherine V. Emerson
Chief Human Capital Officer

FROM: Karen L. Neuman
Chief Privacy Officer

SUBJECT: Strengthening the Culture of Privacy Awareness within the Office of the Chief Human Capital Officer

In light of the January 2014 privacy incident involving the unauthorized disclosure of Social Security numbers by the Office of the Chief Human Capital Officer (OCHCO), I am asking that OCHCO fully implement the attached ten recommendations previously discussed with Executive Director of Human Capital Business Systems Gregg R. Pelowski.

In the aftermath of a 2011 investigation into an OCHCO privacy incident, Privacy Office staff provided additional training to OCHCO senior managers and worked with OCHCO staff to improve the privacy climate. Still, Human Resources Specialists and contractors within OCHCO continue to demonstrate a lack of privacy and Sensitive Personally Identifiable Information (PII) safe-handling awareness, as demonstrated by this most recent incident.

I recognize that OCHCO has experienced a high turnover of personnel on their management teams, and that many of the current managers did not take part in the training and gap analysis conducted in 2012. I also appreciate that you have recently appointed Deputy Chief Human Capital Officer Vicki Brooks as OCHCO's Privacy Point of Contact, and have approached my office about scheduling additional training. Training alone, however, is not going to resolve the privacy issues faced by OCHCO.

I have directed senior staff from my office's Privacy Policy and Advocacy, Oversight, and Compliance Teams to assist OCHCO with implementing the recommendations outlined in the attachment, and have asked Acting Director of Compliance Scott Mathews to lead our efforts in this regard. I have also instructed the Oversight Team to conduct a Privacy Compliance Review in 2015, to assess privacy improvements at OCHCO.

My office will be in touch to schedule a meeting on this matter, and I look forward to working with you to improve the privacy climate at OCHCO.

Thank you.

Attachment

Recommendations

The Office of the Chief Human Capital Office (OCHCO) is the public face of the Department for all new employees and serves a special purpose within DHS. Handling Sensitive Personally Identifiable Information (Sensitive PII)[1] is an essential part of its duties and responsibilities. OCHCO has a special duty to foster trust within DHS and to show employees their privacy and security is taken seriously. The following privacy risks, many of which have already occurred, and corresponding recommendations, show the broad range of privacy incidents facing OCHCO:

1. Unauthorized Access of Information by Visitors/New-Hires: There is a privacy risk that candidate and new hire PII may be viewed by individuals without a need to know during orientation.

   Recommendation: Sensitive PII can only be shared with an individual with a need to know the information in the performance of their official duties. Sensitive PII must be shielded at all times from visitors, guests, and OCHCO employees and contractors who do not have a need to know.

2. Document Management: Documents containing PII are left in plain sight on printers and copiers by OCHCO staff.

   Recommendation: OCHCO should develop policies and procedures for appropriate document management, storage, and disposal. This includes paper and electronic copies.

3. Unauthorized Transfers of Sensitive PII: There is a privacy risk that PII may be e-mailed, either by the candidate or the OCHCO employee or contractor, without appropriate encryption safeguards.

   Recommendation: OCHCO should develop a Standard Operating Procedure (SOP) to memorialize all privacy roles and responsibilities for managers and staff. All OCHCO employees and contractors should be familiar with their roles and responsibilities, including in connection with the SOP.

   Recommendation: OCHCO should develop a policy requiring that all PII transmitted by OCHCO be password-protected or encrypted, whether e-mailed internally or externally. At this time, there is no policy requirement that Sensitive PII sent *within* the Department be password-protected or encrypted.
   Recommendation: OCHCO must follow all existing Department policies regarding the secure transfer of Sensitive PII.

---

[1] DHS defines Personally Identifiable Information (PII) as 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, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. Sensitive PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of these recommendations, Sensitive PII and PII are treated the same.

4. Improper Document Destruction: There is a privacy risk that paper copies of records may be improperly disposed of in a trash can or recycle bin.

   Recommendation: All paper records that contain Sensitive PII should be destroyed in accordance with *DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.* PRIV recommends that the Office of the Chief Security Officer (OCSO) provide on-going training regarding the proper destruction of sensitive documents.

5. Data Integrity: There is a privacy risk that information on employee submitted forms will be manually entered into external databases inaccurately.

   Recommendation: Remind all HR Specialists of the risks that arise when entering data manually into a database. OCHCO should train employees on the importance of accurate data and the inherent risk of manually-entered inaccurate data. OCHCO should develop a policy requiring safeguards to ensure the accuracy of manually entered data such as peer or supervisor review, verification of information with the record subject, or regular system audits.

6. Unauthorized Use of Data: There is a privacy risk that information collected by OCHCO will be accessed or used by someone without a "need to know."

   Recommendation: OCHCO should maintain partitioned shared drives for the different divisions and teams. Processing HR Specialists should not access benefits information on the benefits shared drive and Benefits Specialists should not access processing information, etc.

7. Records Retention: There is a risk that OCHCO will maintain records for a longer period of time than is necessary to complete their mission.

   Recommendation: All OCHCO records have specific record retention schedules on file with the National Archives and Records Administration and catalogued within the *Delegated Examining Operations Handbook.* OCHCO should institute annual "record clean-up" days to ensure they are not retaining information longer than is necessary. Due to the variety of records and corresponding record schedules covering OCHCO records, it is a priority that OCHCO develop and implement a robust records disposal program when records are no longer required.

8. Information Sharing: Most of the information collected, maintained, used, and disseminated by OCHCO is covered by the Privacy Act. As such, information may only be used consistent with the purpose for collection and shared in accordance with published Routine Uses within OPM's SORNs. There is a risk that information will be shared outside of OCHCO for a purpose inconsistent with one of the published Office of Personnel Management (OPM) System of Records Notices (SORN).

   Recommendation: Senior Management with Privacy Act experience should review OPM SORNs prior to the release of information to ensure sharing consistent with the Privacy Act.

Recommendation: OCHCO should develop and Standard Operating Procedure documenting how to share information externally, and internally, consistent with the Privacy Act. This should include an accounting of all disclosures from Privacy Act covered systems.

9. Training: There is a general risk to privacy because OCHCO employees and contractors do not receive on-going, adequate training regarding the safe handling of PII.

   Recommendation: Privacy should be included as a topic in the OCHCO Employee Bootcamp for all new OCHCO hires. OCHCO should launch a communications campaign for new and existing staff and contractors to remind them of their responsibilities in the safe handling of PII and their obligation to comply with DHS Directive 047-01, *Privacy Policy and Compliance*. OCHCO should sponsor on-going privacy awareness training to cover records retention and disposition of documents, safeguarding of PII, reporting of potential or actual compromises of PII and appropriate information sharing with other DHS components and external to DHS.

10. Leadership: There is a privacy risk that OCHCO lacks a dedicated member of the Senior Leadership Team focused solely on privacy, information sharing, and data protection.

    Recommendation: Several Headquarters components have their own dedicated privacy point of contact, including OCHCO's fellow Management line of business, OCSO. Since OCHCO handles a considerable amount of PII, acts as data aggregator for various reporting processes, and engages in bulk information sharing internally and externally, the Privacy Office recommends that OCHCO create or dedicate a member of the senior leadership team for OCHCO-specific privacy policy and training development. At least 50% of this person's time should be dedicated to privacy-related matters.