A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers

FINAL REPORT NO. OIG-24-029-I
JUNE 24, 2024

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

June 24, 2024

MEMORANDUM FOR: Kathi Vidal
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

Jeremy Pelter
Deputy Assistant Secretary for Administration, performing the
non-exclusive functions and duties of the Chief Financial Officer
and Assistant Secretary of Commerce for Administration
U.S. Department of Commerce

FROM: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers*
Final Report No. OIG-24-029-I

Attached is our final report on our evaluation of the United States Patent and Trademark Office's (USPTO's) actions in response to the exposure of domicile addresses. Our objective was to determine whether USPTO complied with federal and U.S. Department of Commerce information technology security standards.

Overall, we found that USPTO leadership did not comply with federal, departmental, and USPTO incident response requirements and knowingly allowed domicile addresses to remain publicly accessible during incident mitigation. USPTO must improve its efforts in safeguarding trademark filers' personal data to rebuild public trust and honor trademark holders' privacy.

Specifically, we found the following:

I. USPTO mishandled required reporting and notification to affected trademark filers after a 3-year exposure of domicile addresses.

II. USPTO leadership allowed domicile addresses to remain publicly accessible after they were aware of the exposure, risking unauthorized disclosures in violation of the Privacy Act.

III. USPTO did not report that additional sensitive personally identifiable information was exposed during the incident or notify affected filers that additional data had been exposed.

IV. The Department Chief Privacy Officer did not assist USPTO in responding to the data exposure.

In its response to our draft report, the Office of the Secretary and USPTO concurred with all 10 recommendations and described both completed and planned actions to address each recommendation. The responses are included in this report as appendix C.

Pursuant to Department Administrative Order 213-5, please submit an action plan that addresses the recommendations in this report within 60 calendar days. We will post the final report on the Office of Inspector General's website pursuant to the Inspector General Act of 1978, as amended (5 U.S.C. §§ 404 & 420).

We appreciate the cooperation and courtesies extended to us by your staff during this evaluation. If you have any questions or concerns about this report, please contact me at (202) 793-2938 or Dr. Ping Sun, Director for IT Security, at (202) 793-2957.

Attachment

cc: David S. Gooder, Commissioner for Trademarks, USPTO
Jamie Holcombe, Chief Information Officer, USPTO
Timothy Goodwin, Chief Information Security Officer, USPTO
Greg Dodson, Deputy Commissioner for Trademark Administration, USPTO
Kathryn Siehndel, Senior Counsel, USPTO
Charles Cutshall, Chief Privacy Officer and Director of Open Government, U.S. Department of Commerce

Report in Brief

June 24, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers

OIG-24-029-I

Background

In June 2023, we learned of the exposure of domicile addresses at the United States Patent and Trademark Office (USPTO) through widespread reporting by the news media. We met with representatives from the Trademarks Organization and USPTO leadership in early August 2023 to gain a better understanding of the incident. We initiated a follow-up review of the actions USPTO took to address the data exposure.

As of December 2023, USPTO managed the registration of more than 3 million trademarks. In recent years, USPTO has detected a rapid increase in potentially fraudulent trademark applications. It has also identified an increase in foreign filings that coincides with the increase in potentially fraudulent trademark applications.

To combat these fraudulent filings, USPTO introduced several safeguards. For example, on August 3, 2019, USPTO implemented the Requirement of U.S. Licensed Attorney for Foreign Trademark Applicants and Registrants, or "the U.S. counsel rule," which requires (1) all filers to provide their domicile address and (2) foreign-domiciled applicants and registrants to have a U.S.-licensed attorney.

Users applying for trademarks provide their personally identifiable information (PII) data—some of which is viewable in the Trademark Status and Document Retrieval (TSDR) system. In February 2023, USPTO determined that domicile addresses in the system had been exposed within publicly accessible web application programming interfaces for 3 years, beginning on February 18, 2020.

Why We Did This Evaluation

Our objective was to assess USPTO's actions in response to the exposure of domicile addresses to determine whether USPTO complied with federal and U.S. Department of Commerce information technology (IT) security standards.

WHAT WE FOUND

USPTO must improve its efforts in safeguarding trademark filers' personal data and sensitive PII. Specifically, we found the following:

I. USPTO mishandled required reporting and notification to affected trademark filers after a 3-year exposure of domicile addresses.

II. USPTO leadership allowed domicile addresses to remain publicly accessible after they were aware of the exposure, risking unauthorized disclosures in violation of the Privacy Act.

III. USPTO did not report that additional sensitive PII was exposed during the incident or notify affected filers that additional data had been exposed.

IV. The Department Chief Privacy Officer did not assist USPTO in responding to the data exposure.

WHAT WE RECOMMEND

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office:

1. Align USPTO policy with departmental requirements to have all USPTO employees report all IT security incidents, including PII exposure, immediately (within 1 hour) once an incident is suspected or confirmed.
2. Establish an internal control process and provide training to ensure all USPTO employees report IT security incidents immediately (within 1 hour) once an incident is suspected or confirmed.
3. Hold USPTO leadership accountable for reporting and notification of IT security incidents in accordance with federal and departmental requirements.
4. Hold USPTO leadership accountable to comply with USPTO risk acceptance policies and procedures.
5. Establish a requirement within USPTO risk acceptance policies and procedures to consider violations of the Privacy Act during IT security incidents.
6. Reassess the non-mission-critical designation of TSDR and other systems supporting the trademark process.
7. Update USPTO policy to meet the federal minimum standard of 2 years and 6 months of log retention.
8. Fully implement log retention controls for USPTO systems according to departmental requirements.
9. Direct the Commissioner for Trademarks to update its applicable System of Records Notice, the *Trademark Manual of Examination Procedure*, and/or its public commitments so that they are all consistent regarding what data will not be publicly viewable.

We recommend that the Deputy Assistant Secretary for Administration:

10. Direct the Office of Privacy and Open Government Director to implement compensating controls and redundant procedures for receiving incidents reported to the Department Chief Privacy Officer.

Contents

Cover: Herbert C. Hoover Building main entrance at 14th Street Northwest in Washington, DC. Completed in 1932, the building is named after the former Secretary of Commerce and 31st President of the United States.

Introduction

As of December 2023, the United States Patent and Trademark Office (USPTO) managed the registration[1] of more than 3 million trademarks.[2] In recent years, USPTO has detected a rapid increase in potentially fraudulent trademark applications. USPTO has also identified an increase in foreign filings that coincides with the increase in potentially fraudulent trademark applications.[3] To combat these fraudulent filings, USPTO introduced several safeguards. For example, on August 3, 2019, USPTO implemented the *Requirement of U.S. Licensed Attorney for Foreign Trademark Applicants and Registrants*, or "the U.S. counsel rule," which requires (1) all filers to provide their domicile address and (2) foreign-domiciled applicants and registrants to have a U.S.-licensed attorney.

Domicile addresses are the applicants' permanent place of residence or the principal place of business (that is, headquarters) of a juristic entity, where senior executives or officers direct and control the entity's activities. USPTO uses the domicile address to confirm whether the applicant is either domiciled in the U.S. or is required to retain authorized, U.S.-licensed representation.

In February 2020, to alleviate stakeholder concerns regarding the U.S. counsel rule's requirement of a domicile address, USPTO updated the trademark application form so that addresses entered into the domicile address fields (hereafter "domicile addresses") would not be viewable by the public. Reflective of this change, USPTO also updated the USPTO-26 System of Records Notice[4] (SORN) Trademark Application and Registration Records[5] to state that USPTO will not make the domicile addresses of trademark filers publicly available. This update to the SORN was published in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a (the Privacy Act), which mandates that a SORN be published in the *Federal Register* that includes the categories of records in the system and the routine uses of the records in the system.

The Privacy Act provides protections for records, which contain information about individuals, that are collected and maintained by the federal government and prohibits the disclosure of such records without the consent of the individual to whom the records pertain, unless an exception applies.

---

[1] Trademark registration gives a company the exclusive right to prevent others from marketing identical or similar products under the same or a confusingly similar mark.

[2] A *trademark* is a symbol, word, or words legally registered or established by use as representing a company or product.

[3] U.S. Department of Commerce (DOC), Office of Inspector General (OIG). August 11, 2021. *USPTO Should Improve Controls over Examination of Trademark Filings to Enhance the Integrity of the Trademark Register*, OIG-21-033-A. Washington, DC: DOC OIG, 1.

[4] A SORN identifies, among other things, the purpose(s) for which information about an individual is collected, from whom and what type of information is collected, how the information is shared with individuals and organizations, and what an individual must do if they want to access and/or correct any records maintained about them.

[5] DOC USPTO. February 18, 2020. *Federal Register Notice.* USPTO-26 Trademark Application and Registration Records (85 Fed. Reg. 8847).

Users applying for trademarks provide their personally identifiable information (PII)[6] data—such as a name, citizenship, domicile address, email address, postal address, telephone number, and attorney information—some of which is viewable in the Trademark Status and Document Retrieval (TSDR) system. In addition to domicile addresses, USPTO committed to keep qualifying email addresses and attorney information from being publicly available to prevent easy consolidation of the data for bad actors who might use it for fraudulent purposes. The TSDR system is used by USPTO and the public to retrieve status information and to view and download documents for pending and registered trademarks. The TSDR system can be used through a user interface such as a webpage or through requests to a web application programming interface (API).[7]

In February 2023, USPTO determined that domicile addresses in the TSDR system had been exposed within publicly accessible APIs for 3 years, beginning on February 18, 2020. This exposure constituted a violation of USPTO's updated SORN and, once USPTO became aware of this exposure, could have contributed to the possibility of unauthorized disclosures of Privacy Act-protected data. In June 2023, we learned of the exposure of domicile addresses at USPTO through widespread reporting by the news media. We met with representatives from the Trademarks Organization and USPTO leadership in early August 2023 to gain a better understanding of the incident. The Trademarks Organization is an office within USPTO and is responsible for trademark examination policy, trademark operations, and trademark administration. Consequently, we initiated a follow-up review of the actions USPTO took to address the data exposure. During our fieldwork, we identified additional findings that warranted an evaluation report.

[6] *PII* is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

[7] An API allows different applications, systems, and devices to communicate with each other and share data. An API request is a message sent to a server asking an API to provide a service or information.

Objective, Findings, and Recommendations

The objective of our evaluation was to assess USPTO's actions in response to the exposure of domicile addresses to determine whether USPTO complied with federal and U.S. Department of Commerce (the Department) information technology (IT) security standards. See appendix A for details on our evaluation scope and methodology.

We found that USPTO mishandled the required reporting and notification to the affected trademark filers after domicile addresses had been exposed for 3 years. We also found that USPTO leadership allowed domicile addresses to remain publicly accessible after they were aware of the exposure, risking unauthorized disclosures in violation of the Privacy Act. Additionally, USPTO did not report that additional sensitive PII was exposed during the incident or notify the affected filers that additional data had been exposed. Lastly, the Department's Chief Privacy Officer (CPO) did not assist USPTO in responding to this incident because of a lapse in the Department reporting process. See appendix B for a timeline of the events discussed in our findings.

USPTO's exposure of trademark filer data may not only reduce public confidence, but also may have equipped bad actors with additional data that could be used to defraud trademark holders. Bad actors could aggregate the pieces of exposed data to convincingly create official-looking USPTO correspondence or impersonate a filer's attorney. Despite these risks, USPTO leadership did not comply with federal, departmental, and USPTO incident response reporting requirements and knowingly allowed domicile addresses to remain publicly accessible during incident mitigation.[8] USPTO must improve its efforts in safeguarding trademark filers' personal data to rebuild public trust and honor trademark holders' privacy.

I. USPTO Mishandled Required Reporting and Notification to Affected Trademark Filers After a 3-Year Exposure of Domicile Addresses

The Department and its operating units are required to adhere to federal privacy law[9] and guidance[10] to ensure that sensitive information, such as PII, is properly safeguarded. USPTO is also required to report confirmed and suspected incidents, as well as notify the affected individuals when an incident occurs. Both the federal government and the Department require that agencies and bureaus (1) report confirmed and suspected incidents

[8] Publicly accessible means that domicile addresses could be viewed on the Internet from anywhere in the world.

[9] The Privacy Act of 1974, as amended, 5 U.S.C §552a.

[10] Office of Management and Budget. January 3, 2017. *Preparing for and Responding to a Breach of Personally Identifiable Information,* M-17-12. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf (accessed February 22, 2024).

immediately,[11] or within 1 hour,[12] and (2) notify affected individuals when an incident occurs.[13]

A. Delays in reporting the incident

On February 24, 2023, after providing support for an earlier customer search request, a Trademarks Organization employee discovered that trademark filers' domicile addresses were available within publicly-accessible APIs. This means that domicile addresses could be viewed on the Internet from anywhere in the world via routine API requests.[14] Ultimately, USPTO determined that domicile addresses in the TSDR system had been exposed for 3 years, beginning on February 18, 2020, which violated the terms of its SORN. The Trademarks Organization employee immediately reported this discovery up the supervisory chain to the Commissioner for Trademarks and the USPTO Chief Information Officer (hereafter "the CIO"). However, the CIO did not report the exposure to the USPTO Security Operations Center (hereafter "the SOC"), USPTO privacy offices, and the Department Enterprise Security Operations Center (ESOC)[15] until March 8, 2023, 12 days later.

This delay in reporting deprived USPTO leadership of the full support from its own SOC and privacy teams when responding to this incident. Reporting incidents to security and privacy personnel as soon as possible is an essential step in the incident response process as these personnel specialize in taking immediate action to mitigate exposure and facilitate notification to appropriate individuals. By delaying reporting to the SOC, all subsequent links in the reporting chain were delayed, including reporting to ESOC, the Department's Office of Privacy and Open Government (OPOG), and the U.S. Computer Emergency Readiness Team (US-CERT).

According to USPTO leadership, they delayed reporting the data exposure to determine the full scope of the incident and to limit knowledge of the exposure until mitigation steps were in place. Additionally, the CIO did not initially consider the privacy aspects of this incident as an actively exploitable vulnerability, but instead approached this incident as a system misconfiguration that needed to be fixed. However, during this incident, the misconfiguration caused the system to be vulnerable to unauthorized access.

---

[11] DOC Office of Privacy and Open Government. *Personally Identifiable Information (PII) Breach Incident Reporting* brochure. https://www.commerce.gov/sites/default/files/opog/pii_incident_reporting_brochure.pdf, 2 (accessed March 28, 2024). The Department requires its operating units to immediately report a suspected or confirmed PII breach incident.

[12] Department of Homeland Security U.S. Computer Emergency Readiness Team. April 2017. *Federal Incident Notification Guidelines*. https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf, 1. This guideline requires agencies to report information security incidents within 1 hour of being identified.

[13] DOC OPOG. September 2022. *United States Department of Commerce Privacy Act (PA), Personally Identifiable Information (PII), and Business Identifiable Information (BII) Breach Notification Plan,* version 7.0.

[14] A *routine API request* is an approved API command used on USPTO webpages as documented in USPTO's TSDR API Syntax.

[15] ESOC manages the Department's network perimeter, compiles data from bureau SOCs, and serves as a liaison to government cybersecurity partners such as the Cybersecurity and Infrastructure Security Agency.

In addition, Trademarks Organization employees did not report the exposure to the SOC because they did not consider it their responsibility to report the exposure of data after informing the CIO of the incident. USPTO's policy[16] of allowing employees 24 hours to report an IT security incident involving PII may have also contributed to the delay in reporting the incident. This USPTO policy does not meet the minimum departmental requirement to report incidents immediately (within 1 hour).

By choosing not to immediately report this incident, the Commissioner for Trademarks and the CIO did not comply with federal, departmental, and USPTO incident response requirements. These delays impeded the security and privacy offices across the Department and USPTO from timely involvement and hindered incident response procedures.

B. Delays in notifying the affected filers

The Department's breach notification plan[17] states that bureaus and operating units must notify individuals whose data was exposed within 30 days or as expeditiously as practicable and without unreasonable delay. However, USPTO did not notify affected trademark filers for more than 3 months (105 days) after discovery of the PII exposure on February 24, 2023. We found that the Trademarks Organization did not begin counting the affected filers until after mitigations were completed on April 1, 2023. Once the mitigations were complete, USPTO started data collection related to domicile addresses and by late April 2023, initially identified approximately 112,000 instances of data entered in domicile address fields. By eliminating duplicate records, the Trademarks Organization ultimately determined that 60,819 individuals had their domicile addresses publicly exposed, and on June 9, 2023, USPTO sent email notifications to those individuals.

USPTO officials explained that it took more than 3 months to notify these individuals because of the complexity of the processes involved. These processes included determining the specific filers affected over the 3-year period, establishing protocol for notifying the 60,819 individuals, drafting the notice, updating ongoing litigation, and setting up a public email inbox for inquiries. By not notifying the affected filers of this incident in a timely manner, USPTO placed them in a more vulnerable state, wherein they were unaware that their domicile addresses could be used for targeted attacks, including in-person solicitation, physical attacks, or fraud via postal mail. Consequently, trademark filers were not able to employ additional protections in response to the public disclosure of their domicile addresses.

[16] DOC USPTO. June 2017. *USPTO Incident Response Plan.*

[17] *United States Department of Commerce Privacy Act (PA), Personally Identifiable Information (PII), and Business Identifiable Information (BII) Breach Notification Plan*, version 7.0, 21.

Recommendations

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office:

1. Align USPTO policy with departmental requirements to have all USPTO employees report all IT security incidents, including PII exposure, immediately (within 1 hour) once an incident is suspected or confirmed.
2. Establish an internal control process and provide training to ensure all USPTO employees report IT security incidents immediately (within 1 hour) once an incident is suspected or confirmed.
3. Hold USPTO leadership accountable for reporting and notification of IT security incidents in accordance with federal and departmental requirements.

II. USPTO Leadership Allowed Domicile Addresses to Remain Publicly Accessible After They Were Aware of the Exposure, Risking Unauthorized Disclosures in Violation of the Privacy Act

From February 18, 2020, to March 8, 2023, unmasked domicile addresses were publicly available through routine API requests. This means that before March 8, 2023, anyone could register for a public API key[18] without being identified and gain access to the exposed data through routine API requests. On March 8, 2023, USPTO implemented firewall rules[19] to block routine public access to the affected APIs. However, these firewall rules did not block all public access to the domicile addresses. On March 10, 2023, the SOC discovered that domicile addresses were still publicly exposed by manipulating USPTO webpage uniform resource locators (URLs)[20] to view them through the still-accessible APIs. Anyone with a basic understanding of webpage content could still view the exposed data without an API key or any form of identification.

In response to the SOC's discovery, the Office of the Chief Information Officer (OCIO) stated that this data exposure via URL manipulation was a risk known to the CIO, and he had accepted the risk to keep the trademark process functioning. The decision to accept the risk, made by the Commissioner for Trademarks and the CIO, allowed domicile addresses to remain publicly accessible from March 8, 2023, to March 31, 2023. However, USPTO leadership did not document this significant decision, or the controls to compensate for this risk, as required by USPTO risk acceptance policy.[21] Furthermore, we found that USPTO's risk acceptance policies do not include specific direction when considering risk for Privacy Act-protected data. The Commissioner for Trademarks' and the

[18] An *API key* is a unique, alphanumeric code used to identify and validate an application or user when using an API.

[19] Firewall rules define how an organization's firewalls should handle inbound and outbound network traffic.

[20] A URL is an address to a webpage. For example, a typical URL could have the form http://www.example.com/index.html. URL manipulation is done when someone alters the URL content in the browser's location bar to probe a website or access "hidden" webpages. URLs are easy to manipulate and often follow a pattern, making them ideal targets for hackers.

[21] DOC USPTO. April 3, 2018. *USPTO IT Policy on Security Risk Acceptance,* version 3.2.

CIO's decision prioritized keeping the system online over security and privacy risks as well as the legal obligation to keep domicile addresses masked from public view.

USPTO leadership stated that they chose not to take the affected APIs offline because it would have "crippled the trademark application process." During this incident, USPTO leadership did not consider the continued exposure of Privacy Act-protected data a sufficient reason to take the system offline. This decision contradicted the TSDR system's categorization as a non-mission-critical system,[22] as well as system security documentation stating that the TSDR system could be taken offline for 48 hours. USPTO leadership repeatedly stated that access to domicile addresses through URL manipulation would violate the system's user agreement. However, the user agreement did not absolve USPTO of its responsibility to protect domicile addresses from unauthorized access through URL manipulation, a basic and well-known technique used by bad actors.

The TSDR system owner stated that on March 8, 2023, TSDR system staff began monitoring the API logs[23] daily to determine if anyone accessed the affected APIs. Apart from the system owner's statements, the TSDR system team could not provide any evidence of daily monitoring or provide any logs from their reviews. The TSDR system team could have created automated triggers, a commonly used mechanism, to alert system staff if the exposed data was accessed. However, the TSDR system owner confirmed that they did not use this capability.

Early in our fieldwork, the SOC provided us with 90 days of a partial log for a single API, which was insufficient to determine how much or how often Privacy Act-protected data was being accessed. We attempted several times to obtain logs relevant to the incident, but USPTO could not provide additional logs. Only after we identified the location of additional logs from system documentation and told USPTO where to find them, did USPTO's cyber team provide us with 6 months of logs from the period of exposure. We found that USPTO had not examined these logs to determine whether Privacy Act-protected data had been inappropriately accessed and potential unauthorized disclosures had occurred.

All the logs provided by USPTO were insufficient to draw firm conclusions about exposed domicile addresses, because of USPTO's misconfiguration of its logs. Despite incomplete logs to conduct our analysis, we found that 12 instances of potential inappropriate access to protected data occurred from February 2023 to March 2023, and 5 of these were potential unauthorized disclosures as they occurred after USPTO leadership knew about the data exposure and chose not to shut down the APIs on February 24, 2023.

[22] A *mission-critical system* is a system that processes any information that the loss, misuse, disclosure, or unauthorized access to or modification of would have a debilitating impact on the mission of the agency.

[23] An *API log* is a record that contains information about API requests, including the timestamp of the API request, the Hypertext Transfer Protocol (HTTP) status code, the command, the universal resource identifier path, the response time, the source IP, the source application, and any log messages.

In addition, the federal audit log retention standard[24] requires USPTO to retain 2 years and 6 months (30 months) of logs. This requirement exists so that a historical record is available for incident responders to determine what happened during an incident. However, we found that USPTO policy,[25] which had not been updated since 2013, requires that logs be retained for only 90 days. The USPTO Chief Information Security Officer agreed that the policy needs to be updated and stated that USPTO plans to do so during the second quarter of FY 2024.

By allowing domicile address data to remain publicly accessible, USPTO leadership's actions were inconsistent with its SORN and risked unauthorized disclosure of Privacy-Act protected data. Amid the unprecedented increase in trademark filing scams, USPTO committed to preventing the domicile addresses from being publicly accessible due to the privacy concerns of trademark filers. USPTO's failure to meet these commitments may cause trademark filers to have concerns about providing their data, which could adversely affect USPTO's ability to carry out its mission.

Recommendations

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office:

4. Hold USPTO leadership accountable to comply with USPTO risk acceptance policies and procedures.
5. Establish a requirement within USPTO risk acceptance policies and procedures to consider violations of the Privacy Act during IT security incidents.
6. Reassess the non-mission-critical designation of TSDR and other systems supporting the trademark process.
7. Update USPTO policy to meet the federal minimum standard of 2 years and 6 months of log retention.
8. Fully implement log retention controls for USPTO systems according to departmental requirements.

[24] Office of Management and Budget. August 27, 2021. M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*.

[25] DOC USPTO. November 5, 2013. *USPTO Network and AIS Audit, Logging, and Monitoring Policy,* OCIO-POL-20.

III. USPTO Did Not Report That Additional Sensitive PII Was Exposed During the Incident or Notify Affected Filers That Additional Data Had Been Exposed

In addition to domicile addresses, other data including attorney information,[26] email addresses,[27] and Internet Protocol (IP) addresses[28] were also exposed during this 3-year period. USPTO's Trademarks Organization did not calculate the number of filers affected by the exposure of this additional data nor did the office consider this number when addressing the incident. If USPTO had included the additional data exposed in its count of affected filers, this incident would likely have exceeded the threshold of a major incident, which requires additional reporting to appropriate congressional committees, Office of Management and Budget's (OMB's) Office of the Federal CIO, and the Department's Office of Inspector General (OIG).[29]

Furthermore, USPTO did not report the exposure of additional data to ESOC or US-CERT, nor did it notify affected filers, because USPTO did not view the additional data as sensitive PII. We found that USPTO privacy officials, as well as the Department CPO, were not told that additional data had been exposed. The SOC was directed to consider only the exposed domicile addresses during the incident. According to multiple sources within USPTO, the Deputy Commissioner for Trademarks and the CIO decided not to report the exposure of attorney information, email addresses, and IP addresses, but to report only the exposure of domicile addresses.

Although some of this additional data may be available from other public sources, USPTO made written and verbal commitments to keep attorney information and email addresses hidden from public view. On April 17, 2020, during a presentation to the Trademark Public Advisory Committee, the Commissioner for Trademarks stated that email addresses would be masked within the TSDR system. The commitments to mask attorney information and email addresses had been reflected in the *Trademark Manual of Examination Procedure* (TMEP) since July 2021, which states that the data will be "hidden from public view"[30] or "will not be publicly viewable."[31] USPTO leadership made these commitments to reduce the opportunities for scammers to misuse the data by contacting trademark owners with

---

[26] Attorney information, when entered in the attorney bar information field, included bar membership number, bar admission year, and state of bar membership.

[27] "Email addresses," when entered in the owner email address field, refer to email addresses of applicants or registrants represented by a U.S.-licensed attorney recognized to practice before the USPTO in trademark matters.

[28] In March of 2023, during the handling of this incident, USPTO acknowledged the intent to mask IP addresses from public view as a security best practice.

[29] OMB. December 2, 2022. M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements.* The definition of a major incident is also defined in the current OMB guidance, M-24-04.

[30] DOC USPTO. July 2021. *Trademark Manual of Examining Procedure*. 602.01(a), "Attorney Identification Information Required." Attorney Identification Information Required. This commitment has remained in subsequent versions, including the November 2023 version.

[31] *Ibid*. 803.05(b), "Email Address." This commitment has remained in subsequent versions, including the November 2023 version.

misleading solicitations for unnecessary legal services or pose as a U.S. licensed attorney to mislead the USPTO.

USPTO stated that it was not legally required to report the exposure of this additional data because the SORN portrays this data as publicly available. However, we found that the SORN had not been updated since February 18, 2020, to account for USPTO leadership statements and the TMEP. For more than 3 years, USPTO has made inconsistent representations to the public regarding its treatment of this additional data through its SORN, a public presentation, and examination procedures. If USPTO intended to not routinely make attorney information, email addresses, and IP addresses publicly available, then USPTO should have revised the language in the 2020 SORN in accordance with subsection (e)(4) of the Privacy Act.

USPTO's decision not to notify affected filers about the exposure of additional data put those filers at risk. The exposure created new channels for bad actors to reach trademark filers. For example, by mining the exposed data, bad actors could then use the exposed data to conduct targeted social engineering attacks against trademark filers. Specifically, a bad actor could combine the additionally exposed data, which may be less sensitive when considered individually, to impersonate a filer's attorney and charge fraudulent fees through either email or postal mail. These communication channels had been compromised; therefore, trademark filers could find it difficult to differentiate between a phishing attack and legitimate USPTO correspondence.

Although USPTO may not have been legally obligated to report the exposure of this additional data, repeatedly exposing sensitive PII and not notifying affected filers may result in a loss of public confidence and trust. In fact, USPTO inadvertently exposed approximately 21,000 private email addresses from the TSDR system in May 2022, which raised privacy concerns within the trademark community. As a result, both this incident and the incident discussed in this report have caused notable disappointment and outrage among some USPTO trademark filers. Repeated exposure of trademark filer data not only reduces public confidence, but also equips bad actors with the data to defraud trademark holders more easily. USPTO must safeguard the sensitive PII of trademark filers.

Recommendation

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office:

9. Direct the Commissioner for Trademarks to update its applicable SORN, the TMEP, and/or its public commitments so that they are all consistent regarding what data will not be publicly viewable.

IV. The Department CPO Did Not Assist USPTO in Responding to the Data Exposure

The Department's Privacy Program is led by the Director of the OPOG, who is also the Department's CPO. One of the responsibilities of the Department CPO is ensuring

effective execution of the Department's breach notification plan. The breach notification plan requires the CPO to thoroughly document all stages of the incident response, ensure routine uses are included within Privacy Act-related SORNs, and assist with all communications with the news media and the public following an incident.

However, we found that the Department CPO was not involved in responding to this incident. The SOC adhered to the Department's procedure to notify the Department CPO about the incident on March 8, 2023. That same day, the SOC also sent a follow-up email including a description of the data exposure incident and corrective actions taken. However, an administrative assistant within OPOG overlooked USPTO's email reports of the incident and did not process them. This resulted in the Department CPO not being aware of the incident until July 6, 2023, after hearing in the news media that the affected filers had been notified of the data exposure. The Department CPO's guidance and expertise could have reduced the amount of time it took to notify the affected individuals by implementing the procedures in the Department's breach notification plan.

This incident revealed OPOG's lack of compensating controls and redundancy in case of human error when receiving notifications of breaches and other incidents. Following this incident, OPOG restructured the administrative assistant position into two dedicated privacy analyst positions. These new positions have updated responsibilities that include reviewing reports of suspected or confirmed incidents, identifying corrective actions, and preparing reports documenting risks and risk mitigation measures.

Recommendation

We recommend that the Deputy Assistant Secretary for Administration:

10. Direct the OPOG Director to implement compensating controls and redundant procedures for receiving incidents reported to the Department CPO.

Conclusion

USPTO has many opportunities to improve its handling of incidents involving the exposure of PII. Complying with federal, departmental, and USPTO incident response requirements should never be treated as optional nor should the decision to allow continued exposure of Privacy Act-protected data be made without full adherence to risk acceptance policies and procedures. Only through taking transparent steps to prioritize the security and privacy considerations of the data entrusted to them by trademark filers will USPTO begin to rebuild public trust.

On April 19, 2024, after the conclusion of our evaluation, USPTO discovered that 14,359 domicile addresses that should have been hidden from public view were inadvertently exposed during the transition to a new IT system. Also exposed during this incident was the bar information of 16,548 attorneys and the email addresses of 33,501 trademark owners. USPTO concluded that this data was exposed between August 23, 2023, and April 19, 2024. A separate incident affecting patents was also detected by USPTO on

March 28, 2024, which exposed the application number and title of the invention between February 5, 2024, and March 29, 2024. Although USPTO took prompt action to report and notify affected individuals of these incidents, we have serious concerns about USPTO's recent history of repeated exposures of sensitive data. These additional exposures reinforce the importance of promptly addressing the recommendations made in this report.

Summary of Agency Response and OIG Comments

On May 17, 2024, we received the Office of the Secretary's and USPTO's responses to our draft report. The Office of the Secretary and USPTO concurred with all 10 recommendations and described both completed and planned actions to address each recommendation. USPTO also provided technical and editorial comments, and where appropriate, we made minor revisions to the final report.

USPTO states multiple times in its response that the additional data exposed during this incident is not "sensitive." However, USPTO also describes its decision to mask this information in certain situations to reduce solicitations and states that data masking efforts are made "to make it harder and/or more costly to bad actors to scrape USPTO data for harmful acts or purposes" and "to protect both itself and the trademark user community against the growing number of trademark scams." USPTO's position that certain owner email addresses and attorney bar information are not sensitive per se appears inconsistent with USPTO's own analysis of the risks of exposing this data, many of which are described in this report. Accordingly, regardless of whether USPTO considers the data to be "sensitive," USPTO should promptly take action to address OIG's recommendations and minimize the risks that it has itself identified.

We have included the Office of the Secretary's and USPTO's responses as appendix C of this report.

We are pleased that the Office of the Secretary and USPTO concurred with our recommendations and look forward to reviewing their proposed evaluation action plan.

Appendix A: Objectives, Scope, and Methodology

Our evaluation objective was to assess USPTO's actions in response to the exposure of domicile addresses to determine whether USPTO complied with federal and Department IT security standards.

To accomplish our objective, we:

- reviewed system-related artifacts, including policy and procedures, planning documents, and security control documentation to determine criteria;
- retrieved, analyzed, and correlated any system logs and other artifacts regarding the TSDR system and related systems; and
- interviewed USPTO officials, including system owners, IT security and operations staff, and management.

We also reviewed compliance with the following applicable internal controls, provisions of law, and mandatory guidance:

- The Privacy Act of 1974, as amended, 5 U.S.C. § 552a
- The Federal Information Security Modernization Act of 2014, as codified at 44 U.S.C. §§ 3551, et seq.
- OMB M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, December 4, 2023
- OMB M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, December 2, 2022
- OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022
- OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, August 27, 2021
- OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017
- US-CERT, *Federal Incident Notification Guidelines,* effective April 1, 2017
- U.S. Department of Commerce, *Enterprise Cybersecurity Policy*, October 2022
- *United States Department of Commerce Privacy Act (PA), Personally Identifiable Information (PII), and Business Identifiable Information (BII) Breach Notification Plan*, September 2022, version 7.0
- *USPTO Incident Response Plan,* June 2017
- *USPTO Network and AIS Audit, Logging, and Monitoring Policy* OCIO-POL-20, revised November 5, 2013

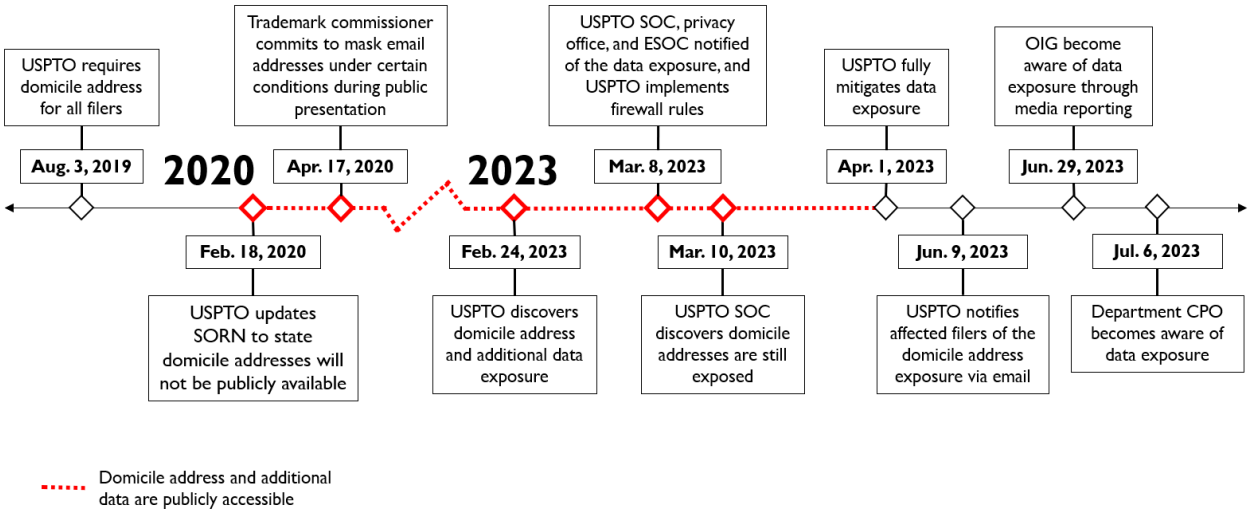
- *USPTO IT Policy on Security Risk Acceptance*, April 3, 2018, version 3.2
- *Trademark Manual of Examining Procedure*, November 2023
- NIST Special Publications 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* September 2020, updated December 2020

Our analysis included the use of computer-processed data, but this data did not materially affect the findings, conclusions, or recommendations. Specifically, we concluded that the TSDR API log data we analyzed portrayed an incomplete record of the API requests during the time period of the logs. We noted the insufficiency of this data in Finding II.

We conducted our evaluation from August 2023 through April 2024 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401-424), and Department Organization Order 10-13, dated October 21, 2020. We performed our fieldwork remotely.

We conducted this evaluation in accordance with *Quality Standards for Inspection and Evaluation* (December 2020) issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that the evidence supporting the evaluation's findings and conclusions should be sufficient, competent, and relevant and should lead a reasonable person to sustain the findings, conclusions, and recommendations. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our review objective.

Appendix B: Timeline of Data Exposure



Source: OIG-generated based upon data exposure events

Appendix C: Agency Response

The Department's and USPTO's responses begin on the following page.

UNITED STATES DEPARTMENT OF COMMERCE
Office of the Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

May 17, 2024

TO: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

THROUGH: MaryAnn Mausser
Commerce GAO/OIG Audit Liaison

FROM: Jeremy Pelter JEREMY PELTER Digitally signed by JEREMY PELTER Date: 2024.05.17 15:56:49 -04'00'
Deputy Assistant Secretary for Administration,
Performing the nonexclusive functions and duties of
the Chief Financial Officer/Assistant Secretary for
Administration

SUBJECT: **Draft Audit Report:** *A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers*

Date: April 17, 2024

Audited Entity: Office of the Secretary

Thank you for the opportunity to respond to the OIG draft report entitled *A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers*. This memo responds to the recommendation for the Deputy Assistant Secretary for Administration. USPTO will respond to the other recommendations.

Title of Finding: IV. The Department CPO Did Not Assist USPTO in Responding to the Data Exposure

- OIG's Recommendation #10: We recommend that the Deputy Assistant Secretary for Administration direct the OPOG Director to implement compensating controls and redundant procedures for receiving incidents reported to the Department CPO.

The Department concurs with the recommendation and, in addition to taking those steps described in the OIG's report, has revised the Department's Breach Notification Plan 2020) to include compensating controls and additional procedures for reporting incidents to the Department's Chief Privacy Officer. The revised plan is under review.

United States Patent and Trademark Office

Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office

May 17, 2024

MEMORANDUM FOR: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation
United States Department of Commerce

FROM: Kathi Vidal
Kathi Vidal
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

SUBJECT: Response to Draft Report, *A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers*

Executive Summary:

We appreciate the work that the Office of the Inspector General Office of Audit and Evaluation (OIG) has done to understand the United States Patent and Trademark Office's (USPTO or Agency) data incident related to trademark files, and we expect that our overall incident reporting process will improve as a result. Data security is paramount, especially when it involves personal information. The USPTO is committed to aligning its data reporting procedures in a way that allows the Department of Commerce (DOC or Department) to meet all federal benchmarks and to holding everyone accountable for following those procedures. We are also invested in ensuring that our organization is equipped to balance the risks inherent in IT solutions with the Agency's obligation to continue its operations and enable stakeholders to protect their valuable intellectual property. The OIG's recommendations will help inform that balance going forward.

The Agency works hard to alert trademark users that the data they include in trademark applications, even personally identifiable information, will be made public. Because trademark registrations involve property rights, the Agency is required to include contact information in the public file for the purpose of private disputes, and customers must expressly acknowledge that they have no right of confidentiality in the data they include in trademark filings. However, the Agency has made certain decisions to mask data in connection with its evolving fraud prevention efforts. As the USPTO works with the OIG to implement its recommendations, it is simultaneously committed to combatting the rising fraudulent activity plaguing the trademarks community. While the Agency cannot prevent the activities of a growing population of bad actors that engage in fraudulent filings (submitted to the USPTO) and fraudulent solicitations (targeting the trademark user community), it can establish roadblocks. Masking data from certain data sets – even though this data is not sensitive, and generally considered part of a public trademark filing – was one attempt to make it harder and/or more costly for bad actors to scrape USPTO data for harmful acts or purposes. To the extent there may be tension between the OIG's recommendation related to certain data masking and the Agency's ability to deploy

fraud prevention, we are confident that we can come to a resolution that best protects our trademark user community and satisfies the OIG's goals. As the USPTO continues to evaluate the utility of certain fraud measures (including data masking), it will consult its Trademark Public Advisory Committee (TPAC) and the trademark user community to get their input.

Response to Recommendations:

The OIG issued nine recommendations to the USPTO, listed below, followed by the USPTO's responses.

Recommendation 1: *Align USPTO policy with federal and departmental requirements to report IT security incidents involving PII within 1 hour.*

USPTO Response: The USPTO concurs. The USPTO will ensure that its Breach Notification Policy, OCIO-POL-17, is updated to instruct employees to report discovery of any suspected incident *immediately* to the Office of the Chief Information Officer (OCIO) Security Operations Center (SOC) and their supervisor, which mirrors the DOC *Privacy Act (PA), Personally Identifiable Information (PII), and Business Identifiable Information (BII) Breach Notification Plan*.

Recommendation 2: *Establish an internal control process and provide training that emphasizes that all USPTO employees must report IT security incidents, including PII exposure, within 1 hour.*

USPTO Response: The USPTO concurs. The recommendation to establish an internal control process and provide training is well-aligned with the USPTO's updates to its Breach Notification Policy and the forthcoming revisions to OCIO's "The Rules of the Road" (USPTO Agency-wide policy on using information systems). These planned updates already mandate immediate incident reporting, including reporting of personally identifiable information (PII), by all employees and contractors. The ongoing enhancements to our annual cybersecurity awareness training, and the integration of automated technical controls within the information technology (IT) service desk system, are steps we are actively taking to ensure compliance and expedite incident reporting processes. These measures collectively support the requirement for reporting IT security incidents within one hour, reinforcing our commitment to robust security practices and regulatory compliance.

The Agency currently mandates IT Security Awareness Training for all employees and contractors every year. For 2024, the USPTO had a 100% completion rate across the Agency. For the FY25 IT Security Awareness Training, the USPTO will highlight the requirement to report any suspected or actual cybersecurity incidents, including PII, immediately to the SOC and their supervisor.

The USPTO is also establishing internal controls through service desk operations that will ensure security and privacy related incidents are reported in accordance with established polices.

Recommendation 3: *Hold USPTO leadership accountable for reporting and notification of IT security incidents in accordance with federal and departmental requirements.*

USPTO Response: The USPTO concurs. All Agency leaders are responsible for adhering to all Agency data security policies and requirements. The Agency will continue to consider any failures to adhere to these policies and address them as necessary, consistent with all relevant employment laws and policies.

Recommendation 4: *Hold USPTO leadership accountable for complying with USPTO risk acceptance policies and procedures.*

USPTO Response: The USPTO concurs. All Agency leaders are responsible for following risk acceptance policies. The Agency will continue to consider any failures to adhere to these policies and address them as necessary, consistent with all relevant employment laws and policies.

The Agency fully recognizes the importance of ensuring that its risk acceptance procedures are updated (see Response to Recommendation 5 below) and adhered to, and appreciates that the OIG's evaluation has triggered policy improvements. As an additional note, the OIG's findings do not recognize the effective risk management efforts applied to this incident. Setting aside the delay in reporting to the Department which the USPTO will rectify moving forward, in this situation the relevant USPTO executives evaluated the type and potential harm to affected individuals, acknowledging evidence that the incident was accidental and there was no evidence of data misuse. The executives determined that the harm level was low, based on the security controls, the sensitivity of the exposed data, and the duration of exposure. USPTO executives also had to consider the level of harm to the entire trademark community if the incident had been disclosed before it was remedied. The fact that the incident remained unknown publicly for an extended period of time until it was internally discovered further supported the low risk of harm conclusion. That said, the USPTO acknowledges risk management practices and procedures can be enhanced in our executive ranks and is committed in doing so through education and training.

Recommendation 5: *Establish a requirement within USPTO risk acceptance policies and procedures to consider violations of the Privacy Act during IT security incidents.*

USPTO Response: The USPTO concurs. In practice, it already considers violations of the Privacy Act when evaluating the risks related to IT security incidents. But the Agency recognizes that its written risk acceptance materials do not currently capture this element. The OCIO will update the IT Policy on Risk Acceptance to ensure violations of the Privacy Act are considered when making risk determinations and memorialized in writing.

Recommendation 6: *Reassess the nonmission-critical designation of TSDR and other systems supporting the trademark process.*

USPTO Response: The USPTO concurs and has reassessed the designation of the Trademark Status & Document Retrieval (TSDR) system. In its report, the OIG states that the USPTO's decision to leave the TSDR accessible while fixing the impacted application programming interface (API) contradicted

the TSDR system's categorization as a "nonmission-critical system." However, this assessment overlooks the USPTO's active evaluation of the risk associated with the incident and the criticality of the TSDR to trademark users.

The OIG defines a mission-critical system as "a system that processes any information that the loss, misuse, disclosure, or unauthorized access to or modification of would have a debilitating impact on the mission of the agency." In its discussions with the OIG, it appeared that the OIG's use of "nonmission-critical designation" refers to the USPTO's determination that the TSDR is not a "High Value Asset" (HVA) for purposes of national government continuity. The USPTO recently evaluated all of its IT systems in coordination with the DOC to determine which systems constituted HVAs. The USPTO has re-evaluated the TSDR system against the DOC High Value Assets checklist and has confirmed that the TSDR does not meet the criteria established under OMB M-19-03, "Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program." That said, the TSDR, along with certain other USPTO systems, enable the USPTO to carry out its mission of granting patents and registering trademarks to stakeholders. The ability for the USPTO to meet its obligations to the public remains a critical factor in the overall planning of how best to mitigate an incident or suspected incident.

In its decision to leave the TSDR online while continuing to correct the incident related to applicant domicile addresses, the executives had determined that the likelihood of access of domicile addresses was very low. Any typical user of USPTO systems would *not* have encountered viewable domicile addresses while interacting with the TSDR. The specific TSDR API where domicile information was inadvertently left unmasked is used to retrieve media files. A user would have to suspect that domicile information was unmasked (when it usually is not) and take additional steps to retrieve unmasked application information. Understanding the unlikely exploitation of this deeply-buried vulnerability, relevant USPTO executives weighed the risks and only then decided to not shut down the TSDR while remediating the vulnerability.

The TSDR contains all application and registration records including the official letters that tell applicants what steps they must take by a certain date to achieve registration and avoid their applications being abandoned. If the TSDR had been taken offline, applicants would not have had access to their application information and official letters, and could have easily missed response deadlines. In deciding to keep the TSDR online, the Agency weighed the low risk of potential exposure of domicile addresses with a) the significant risk of halting trademark filing activity, and b) the risk of alerting scammers to a potential weakness in the system, (considering that the USPTO would have had to explain to the user public why it was taking down such a critical system).

Recommendation 7: *Update USPTO policy to meet the Department's minimum standard of 2 years and 6 months of log retention.*

USPTO Response: The USPTO concurs. In September 2023, the USPTO updated the OCIO's Comprehensive Record Schedule (CRS) to include requirements from OMB-21-31 for retaining IT and Cybersecurity logging events for 30 months. It will also update the OCIO's Audit, Logging, and Monitoring Policy in a version to be released in FY24

Recommendation 8: *Fully implement log retention controls for USPTO systems according to departmental requirements.*

USPTO Response: The USPTO concurs and will take every reasonable measure to ensure that the log retention controls are met.

Recommendation 9: *Direct the Commissioner for Trademarks to either update the Trademark Application and Registration Records SORN or update the TMEP so that they are consistent with USPTO's public commitments to make certain data non-publicly viewable.*

USPTO Response: The USPTO concurs with the OIG's recommendation to update the Trademark Manual of Examination Procedure (TMEP) to ensure that users understand how and when their data is disclosed. Over the next several months, the USPTO will evaluate how to update the TMEP to ensure even more transparency to the trademark system users and consistency with our Privacy Act commitments. In addition, the USPTO will consider a broader discussion with its TPAC and the public about how it can continue to bolster its fraud prevention efforts, while working with current IT systems.

The data to which this recommendation refers are: (1) owner email addresses and (2) attorney bar information, neither of which are considered sensitive. Because trademark registrations involve property rights, the Agency is required to include contact information in the public file for the purpose of private disputes, and the USPTO works hard to make this clear to the users. The Privacy Act System of Records Notice (SORN) covering "Trademark Application and Registration Files" (SORN 26) tells users that all contents of trademark files, except for domicile addresses, will be publicly disclosed. In addition, users of the TSDR are told that all of the information in their application files, except domicile addresses, will be made public. In fact, users must expressly acknowledge that they have no right of confidentiality in the data they include in trademark filings.[1] If they forget the contents of the confidentiality acknowledgement, they can visit the Trademarks Organization's public page on how it uses trademark filing information.[2]

Those seeking trademark registrations are offering goods or services for sale in U.S. commerce. The owner email addresses provided to the USPTO are those used as part of their business. Similarly, attorney bar information is routinely accessed in public databases by prospective clients or opposing

---

[1] Upon submission of any application for trademark registration, users must acknowledge the following: "*All information you submit to the USPTO at any point in the application and/or registration process will become public record, including your name, phone number, email address, and street address. By filing this application, you acknowledge and agree that YOU HAVE NO RIGHT TO CONFIDENTIALITY in the information disclosed. The public will be able to view this information in the USPTO's on-line databases and through internet search engines and other on-line databases. This information will remain public even if the application is later abandoned or any resulting registration is surrendered, cancelled, or expired. To maintain confidentiality of banking or credit card information, only enter payment information in the secure portion of the site after validating your form. For any information that may be subject to copyright protection, by submitting it to the USPTO, the filer is representing that he or she has the authority to grant, and is granting, the USPTO permission to make the information available in its on-line database and in copies of the application or registration record.*"

[2] www.uspto.gov/trademarks/apply/faqs-personal-information-trademark-records

litigants to determine the legitimacy of attorney credentials. However, in response to a few comments in public rulemaking on electronic filing and U.S. counsel requirements, the USPTO determined that it would mask certain owner email addresses where owners are represented by counsel, and attorney bar information, in some of its systems in order to make it harder for the data to be scraped for solicitation purposes, not because the data is private. The Agency memorialized this in the TMEP in July 2021.

The USPTO does not view unrepresented owner email addresses as any more or less private than those who are represented by counsel. Rather, the standard is that this information *is* appropriate for public disclosure, and even if hidden, it may become public at any moment, should one's counsel withdraw or be disciplined. It is critical for users to understand that owner emails may be used for contact purposes, and the USPTO suggests to users that they may want to create separate emails for their trademark filings.[3] Similarly, attorney bar information is squarely designed for public use; it is published by almost every state bar and required on public court filings. It is also only masked if attorneys enter it into a certain spot on the trademark filing, not when it is entered elsewhere in the filing. Even though the TMEP provides transparency into the USPTO's internal masking approach for some email addresses and bar information, the USPTO purposely communicates in SORN 26 that this information will be part of the public files, because that is often the case. The Agency works hard to alert trademark users that the data they include in trademark applications, even PII, will be made public. That said, the USPTO acknowledges that the TMEP's statements about masking the owner emails and attorney bar information may lead to some confusion.

As a directly related matter, the USPTO is working to protect both itself and the trademark user community against the growing number of trademark scams. It currently keeps the public abreast of known scams related to PII,[4] provides examples of fraudulent solicitations customers have received,[5] and advises on tips to prevent against trademark scams specifically.[6] The masking of some owner email addresses and attorney bar information prescribed by the TMEP is directly related to these fraud prevention efforts, whereby the Agency is masking data in certain locations as a courtesy to avoid some data-scraping by bad actors. The Agency cannot prevent bad actors from using trademark owner contact information, which in many instances must be published. But it can implement hurdles to make some of that data collection more difficult.

Fraud prevention is an evolving effort at the USPTO. We are continuing to evaluate the utility of certain measures, including the data masking of email addresses and attorney bar information in certain systems. In implementing the OIG's recommendation, the Agency intends to consult with its TPAC and modify the TMEP to resolve any confusion about the confidentiality that data.

---

[3] The USPTO webpage "Personal information in Trademark records" states: "With respect to a trademark owner's email address, although the email address provided with a trademark filing will be publicly viewable, you could create an email address specifically for communication and correspondence with the USPTO for trademark filings related to an application or registration. This will help you avoid receiving unsolicited communications and spam at your personal or business email address."

[4] See "Recognizing common scams" webpage: www.uspto.gov/trademarks/protect/recognizing-common-scams

[5] See "Examples of fraudulent solicitations" webpage: www.uspto.gov/trademarks/protect/examples-fraudulent-solicitations

[6] See "Protect against trademark scams" webpage: www.uspto.gov/trademarks/protect

Conclusion

In closing, the USPTO appreciates your work and thanks the Assistant Inspector General for Audit and Evaluation for providing us with this report. The USPTO continues its work to improve data security and reporting processes and drive the best outcomes on behalf of its trademark user community. These findings will help the USPTO achieve those goals and create a work environment of excellence. The USPTO's Office of the Chief Information Officer and the Trademarks Organization have made, and will continue to make, improvements to implement the report's recommendations, and we are confident in our abilities to satisfy these recommendations in timely manner. The USPTO looks forward to working with your office in the future as we continue our efforts.

USPTO Technical Comments to OIG Draft Report:

"A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers"

Page 1, paragraph 3, first sentence should be amended to replace "public backlash caused by the newly implemented U.S. counsel rule," with "*stakeholder concerns regarding the U.S. counsel rule's requirement of a domicile address.*" The general public did not contact the USPTO to raise concerns about the US counsel rule or the domicile address provisions. Some stakeholders did raise concerns about privacy with regard to the domicile requirement, and others raised concerns in rulemaking about third party misleading solicitations related to owner email addresses and attorney bar information.

Page 1, paragraph 3, first sentence should be amended after "updated the trademark application form so that…" and add "*applicants had the option of providing two addresses, one mailing address and one domicile address. The USPTO announced that domicile address would be masked and not publicly available only where the applicant provided a different mailing address and the domicile address was entered in the domicile address field.*" Delete the remainder of the original sentence that reads "domicile addresses would not be publicly available."

See TMEP 601.01(e) Hiding the Domicile Address

> *"Most TEAS forms allow an applicant or registrant to specify the owner's mailing address, which is publicly viewable, and a separate domicile address, which is masked or hidden from public view. If the applicant or registrant provides the same address as its mailing address and domicile address in those forms, the address will be viewable by the public. To hide the applicant's or registrant's domicile address from public view, the applicant or registrant must provide a mailing address that differs from its domicile address and enter the domicile address into the dedicated "Domicile Address" fields on the Owner Information page within most TEAS forms.*
>
> *If an Office action is being issued that questions the validity of a domicile address that was hidden from public view, an examining attorney or post-registration examiner must not list the exact address in the Office action. However, if evidence is being attached to the Office action to support the inquiry, an examining attorney may attach evidence that identifies the address if necessary. Applicant may then later petition the USPTO to have that information redacted."*

Page 1, paragraph 3, second sentence should be amended after "trademark filers" to add "*who provided their domicile address in the domicile address field publicly available.*"

Page 2, first paragraph, second sentence should be amended to add "*in order to prevent easy consolidation of the data for data scrapers who might use it for fraud purposes"* at the end of the sentence. Also, "attorney information" should be amended to say "*attorney bar information.*" The attorney names and correspondence addresses are publicly available.

Page 2, second paragraph, fourth sentence should replace "the Trademark Office" with "*the Trademarks Organization.*"

Page 2, second paragraph, fifth sentence should replace "the Trademark Office" with "*the Trademarks Organization*." Every time it appears in the report, the reference to "the Trademark Office" should be changed to "*Trademarks Organization*" or "*Trademarks*." Similarly, references to "*USPTO*" should be amended to "*The USPTO*" everywhere it appears.

USPTO Technical Comments to OIG Draft Report:

"A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers"

Page 3, third paragraph, first sentence, should be amended to delete the phrase "*but also may have equipped bad actors with the data that could be used to defraud trademark holders*." For many years prior to 2019, bad actors have been using all available data fields to solicit trademark holders into paying for unnecessary legal services including publicly available mailing addresses and phone numbers.

Page 3, third paragraph, second sentence, should be deleted. For many years prior to 2019, bad actors have been using all available data fields to solicit trademark holders into paying for unnecessary legal services including publicly available mailing addresses and phone numbers.

Page 4, first full paragraph, first sentence, should be amended to read "*On February 24, 2023, after providing support for an earlier customer search request, a Trademark Office employee discovered that trademark filers' domicile addresses were available within publicly-accessible TSDR APIs.*" The correspondence in question did not pertain to exposed data or the TSDR, and the initial email is attached.[1]

Page 4, first full paragraph, second sentence should be amended to read: "*This means that domicile addresses could be viewed on the internet from anywhere in the world if the user had reason to know the internal USPTO API command to call up a specific trademark document.*"

Page 4, third paragraph, second sentence should be amended to read: "*Additionally, while the CIO considered the privacy aspects of this incident, it approached this incident as a system misconfiguration that needed to be fixed.*" The USPTO considered the privacy aspects of this incident in light of the fact that a user would have to know the internal USPTO API command to call up a specific document, which is unlikely.

Page 5, third full paragraph, third sentence should be amended to delete reference to "o*r fraud via postal mail.*" The mailing address for each individual remained publicly available and that mailing address would be considered postal mail.

Page 6, second paragraph, first sentence should be amended to add "*for a user that specifically researched the internal USPTO API commands to call up a specific trademark document.*" The USPTO understands OIG's use of "routine API request" as IT parlance but wants to make clear that there would have been nothing routine about an individual knowing and using the USPTO's internal access code.

Although the report calls it a routine API request, the user would have to go through many steps to access the domicile of a specific file or group of files. They would have to know the trademark application serial number in order to retrieve the application document ID in the TSDR API. From there, the user would have to make an API call for the media file from a specific initial application and then go back into the API to request the domicile information from that file. Programmatically, that is not "routine" for an ordinary user.

Mail - TEAS - Outlook.pdf

1

USPTO Technical Comments to OIG Draft Report:

"A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers"

Page 8, second paragraph, second sentence, delete "*due to concerns about the unprecedented increase in trademark filing scams*." We began masking domicile addresses for those applicants who provided both a mailing address and a domicile address because users requested this for privacy reasons. We did not mask this data out of concerns for filing scams.

Page 9, first partial paragraph, first sentence, should delete "USPTO's Trademark Office did not calculate the number of filers affected by the exposure of this additional data" and amend the rest of the sentence accordingly. The domicile information was derived from the data set including all filings potentially affected.

Page 9, first full paragraph, fourth sentence should be amended to add "*because they did not view the additional data as sensitive PII*" at the end of the sentence.

Page 9, second full paragraph, first sentence should be amended to add "*when entered in the attorney bar information field and the owner email address field for a represented party*." See TMEP 803.05(b) and 811.01[2] which both highlight that the data will not be publicly viewable when it is entered into the appropriate data field. The USPTO did not indicate that we would mask that data wherever it appears in the records.

Page 9, second full paragraph, second sentence, should be amended to add the word "*Deputy*" before "Commissioner" and add "*some owner*" before "email addresses." The TPAC comments[3] as well as the TMEP Section 803.05(b) made clear that:

- "*The email address listed in the owner field for trademark applicants who are represented by a qualified U.S. attorney will not be publicly viewable."*
- *"The email address listed in the owner field for trademark applicants who are not represented by a qualified U.S. attorney will be used by the USPTO for correspondence and will be publicly viewable as the correspondence email address."*

Page 9, second full paragraph, third sentence should be amended to replace "data will be hidden from public view or will not be publicly viewable" to "*some owner email addresses provided in the owner email address fields will not be publicly available and attorney bar information entered into the bar information field will be hidden from public view*." Only those email addresses for a represented party will be not publicly viewable and if the attorney withdraws or is revoked, or the attorney is removed

[2] TMEP 811.01 says "Bar information entered in the bar information fields on the attorney information page will be hidden from public view."

[3] Voice over from Ms. Meryl Hershkowitz (Deputy Commissioner for Operations and previous Acting Commissioner) at the 17 April 2020 TPAC public meeting: "*And I'm happy to say that in the upcoming weeks, we will be masking the owner email address field in TEAS and TEASi documents viewable in TSDR for our filing system for the outside user. We will also be masking the submissions viewable, not only in the documents tab of TEAS, but in all programming – all application programming interfaces for APIs and also in the PDF downloads. After the deployment, you'll see four Xs in the owner email address field when you open a TEAS or TEASi document in TSDR. Providing an email address for the owner in any other field, however, will be public, so please be careful. Unrepresented owner email addresses will still be viewable in the correspondence email field*."

from the record due to misconduct, the owners' email address then automatically becomes publicly viewable as the correspondence email address.

Page 9, second full paragraph, fourth sentence should be amended to say "*USPTO leadership made these commitments to reduce the opportunities for scammers to misuse the data by contacting trademark owners with misleading solicitations for unnecessary legal services or pose as a U.S. licensed attorney to mislead the USPTO.*" This statement is factually wrong. The USPTO has never stated that the reason for masking owner email addresses and attorney bar information was to reduce fraudulent filings and protect privacy because those were not the reasons for masking that data. We masked the data because scammers scrape those data fields to solicit trademark applicants for unnecessary legal services or to pose as a U.S. licensed attorney to circumvent USPTO rules.

REPORT

FRAUD & WASTE & ABUSE

HOTLINE

Department of Commerce

Office of Inspector General Hotline

www.oig.doc.gov | 800-424-5197