Office of Intelligence and Analysis
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 9, 2024

ACTION

TO: (b) (6), (b) (7)(C)
Acting Director, Transparency and Oversight Program Office

FROM: Kenneth Wainstein (b) (6)
Under Secretary for Intelligence and Analysis

SUBJECT: **Mitigation Measure for Preliminary Inquiry No. 2023-03**

I have reviewed the Preliminary Inquiry Report for Preliminary Inquiry No. 2023-03, which found that a technical error by an I&A developer in the Directorate of Technology and Data Services inadvertently provided access to the Homeland Security Information Network Intelligence Community of Interest (HSIN-Intel) for individuals not approved to access HSIN-Intel. The report also found apparent discrepancies in I&A personnel's understanding as to what constitutes personally identifiable information (PII) when submitting analytic products for inclusion in the Homeland Security Information Network (HSIN). The Intelligence Oversight Officer (IOO) further found that confusion over the difference between the terms PII, sensitive PII (SPII), and U.S. persons information (USPI) is a recurrent issue with which their office is regularly confronted. In light of these observations, and after considering the measure recommended by the Acting Director of the Transparency and Oversight Program Office to mitigate the likelihood that similar issues recur, I request that the D/TOPO implement the following action upon my signature above:

> The D/TOPO, in coordination with the Chief of Staff, will prepare a message educating the I&A workforce on the differences between PII, SPII, and USPI.

I further request that the IOO report to me on the status of this request upon its completion or no later than six months from the date of this memorandum, whichever occurs first, and that the IOO transmit a copy of this decision memorandum and associated preliminary inquiry report to the DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties.

cc:

Avery Alpha, Principal Deputy Under Secretary for Intelligence and Analysis
Adam Luke, I&A Chief of Staff
Jim Dunlap, Deputy Under Secretary for Analysis
Stephanie Dorsey, Deputy Under Secretary for Collection
David Carabin, Deputy Under Secretary for Partnerships
(b) (6), (b) (7)(C), Acting Deputy Under Secretary for Management
(b) (6), (b) (7)(C), Senior Advisor to the Under Secretary for Intelligence and Analysis and Director, Intelligence Enterprise Program Office
(b) (6), Chief Privacy Officer
(b) (6) Officer for Civil Rights and Civil Liberties
Matthew Kronisch, Associate General Counsel for Intelligence

Office of Intelligence and Analysis
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 9, 2024

MEMORANDUM FOR THE UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS

FROM: (b) (6), (b) (7)(C)
Acting Director, Transparency and Oversight Program Office

SUBJECT: **Mitigation Recommendation for Preliminary Inquiry No. 2023-03**

Purpose: To solicit your approval of one recommendation in light of the results of the Intelligence Oversight Officer (IOO)'s Compliance Inquiry No. 2023-03, which found that a technical error by an I&A developer in the Directorate of Technology and Data Services (TDS) inadvertently provided access to the Homeland Security Information Network Intelligence Community of Interest (HSIN-Intel) for individuals not approved to access HSIN-Intel. The IOO also found apparent discrepancies in the understanding of I&A personnel as to what constitutes personally identifiable information (PII) when submitting analytic products for inclusion in the Homeland Security Information Network (HSIN).

Background: As set forth in greater detail in the attached Preliminary Inquiry Report for Inquiry No. 2023-03 **(Attachment B)**, the IOO concluded that a coding error resulted in 439 I&A products being improperly accessed by HSIN users (b) (5) [redacted] With respect to this coding error, I defer entirely to the findings and recommendations of TDS in its after action report and have no recommendations with regard to how to prevent or mitigate such errors in the future.

The IOO did, however, note multiple instances of products being marked in HSIN as containing no PII when, in fact, they did contain PII. These discrepancies complicated the IOO's assessment of the privacy implications of the coding error because they could not rely on the authors' assertions as to whether a product contained PII. The IOO further observed that confusion over the difference between the terms PII, sensitive PII (SPII), and USPI is a recurrent issue with which their office is regularly confronted.

To mitigate the likelihood of this issue recurring, I recommend that you direct the following:

The Acting Director of the Transparency and Oversight Program Office, in coordination with the Chief of Staff, will prepare a message educating the I&A workforce on the differences between PII, SPII, and USPI.

Clearance: This memorandum has been cleared by the Principal Deputy Under Secretary for Intelligence and Analysis. The Office of the General Counsel's Intelligence Law Division has reviewed this memorandum and has no legal objections concerning it.

Timeliness: To ensure implementation of the mitigation measure recommended above, I request that you indicate your approval or disapproval of the recommendation in the attached action memorandum **(Attachment A)** by [THREE WEEKS FROM DATE OF FINAL SUBMISSION.]

Attachment(s):
A. Draft Memorandum, *Mitigation Measures Concerning Preliminary Inquiry No. 2023-03*
B. Preliminary Inquiry Report for Inquiry No. 2023-03.

Office of Intelligence and Analysis
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 28, 2024

MEMORANDUM FOR THE UNDER SECRETARY OF INTELLIGENCE AND ANLYSIS

FROM: (b) (6), (b) (7)(C) [redacted]
Intelligence Oversight Officer

SUBJECT: **Preliminary Inquiry No. 2023-03**
Factual Findings & Compliance Determination

Under Appendix A to I&A Instruction No. IA-1000, *Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines* (January 19, 2017) ("IO Program"), I am required to commence a preliminary inquiry upon notification of any potential violation of Federal criminal law or questionable activity.[1] A preliminary inquiry is an administrative fact-finding process conducted by I&A's Privacy and Intelligence Oversight Branch (PIOB) to determine whether a questionable activity constitutes a violation of applicable law, executive order, directive, regulation, agreement or arrangement, policy, or provision of the Guidelines. This report documents my factual findings and compliance determination for Preliminary Inquiry No. 2023-03, which concerned unauthorized access of Homeland Security Information Network (HSIN) Communities of Interest (COI) HSIN-Intelligence (HSIN-Intel) intelligence products between March 15 and May 11. This memorandum is submitted to you in furtherance of my obligation to "[r]eport[] the results of preliminary inquiries concerning all questionable activities to the USIA and the Associate General Counsel for Intelligence [AGC/ILD] for referral, as appropriate, to the Inspector General, the Chief Security Officer, the President's Intelligence Oversight Board, and the Congress."

As set forth in greater detail below, I have concluded that a technical error by an I&A Directorate of Technology and Data Services (TDS) developer inadvertently changed HSIN-Intel from a limited access group to an "everyone" group - providing access to HSIN-Intel's library of intelligence products to all HSIN users, including those not approved for access to the HSIN-Intel. (b) (5) [redacted]

[1] A Questionable Activity is any conduct related to an intelligence activity reasonably believed to constitute a violation of any applicable law, executive order, presidential or other directive, regulation, international or domestic agreement or arrangement, or applicable national or departmental policy, including, but not limited to, the requirements of IA-1000 with respect to I&A personnel.

Our review also indicated that I&A's privacy practices would benefit from additional clarification or training as to what constitutes U.S. Person Information (USPI) and/or Personally Identifiable Information (PII), as I&A authors and/or reviewers may not consistently be labeling their products properly while uploading them into HSIN-Intel. A common misconception among I&A personnel that my team regularly encounters and corrects in our informal oversight consultations is that only *sensitive* PII (such as social security numbers) constitutes PII. In reality, the mere inclusion of a name in a product, even if the name is publicly available, constitutes PII.

A. Background

HSIN is the Department of Homeland Security's (DHS) official system for trusted sharing of Sensitive But Unclassified (SBU) information between federal, state, local, territorial, tribal, international, and private sector partners. HSIN has multiple COIs with unique requirements for membership and access. One of these COIs is HSIN-Intel. Managed by DHS I&A, HSIN-Intel provides the homeland security enterprise with a secure platform for collaboration and sharing of SBU information, data, products, analytical exchange, and situational awareness. To become a member, HSIN-Intel requires individuals to be vetted intelligence professionals from a government agency with homeland security, intelligence, and/or law enforcement responsibilities in accordance with the HSN-Intel Charter. On March 15, an I&A contract developer accidently modified the HSIN-Intel permissions allowing HSIN members without authorization to access HSIN-Intel. The error was discovered by the Program and Performance Evaluation (PPE) team during a customer usage assessment. After the Office of Chief Information Officer (OCIO) and the OCIO Solution Development Division (SDD) were notified, the error was corrected on May 11. The error led to the unauthorized access of HSIN-Intel products between March 15 and May 11.

As described below, some of the HSIN-Intel products viewed contained either USPI or PII. These are two terms that arise from two different legal/policy frameworks and are defined differently, although there is some overlap between the two. USPI refers to information about a U.S. Person (USPER) as defined in I&A's IO Guidelines in furtherance of EO 12333. A USPER could be an individual U.S. citizen, a Lawful Permanent Resident, a corporation, or an unincorporated association (e.g., Proud Boys, Hell's Angels).

The term "PII," by contrast, is derived from a number of privacy laws and regulations, many of which are implemented and enforced by the DHS Office of Privacy (PRIV). That term only applies to natural individuals. The term may or may not include PII on non-U.S. persons, depending on the law or policy being enforced. Thus, some USPI may not be PII, and some PII may not be USPI.

B. Factual Findings

Fact-finding process

As per the I&A TDS After Action Report (AAR), the coding error was discovered on May 9 and conveyed to the HSIN-Intel Project Management Officer (PMO), who worked with

I&A TDS and OCIO to correct the error on May 11. The AGC/ILD determined that the incident met reporting thresholds for immediate reporting to the Intelligence Oversight Board (IOB) as a potentially significant or highly sensitive matter and provided the required IOB report on May 12 via email. In this email, the AGC/ILD noted, *inter alia*, that (b) (5) [redacted]

The Acting Director of the Transparency and Oversight Program Office (D/TOPO) informed me that PRIV needed to first investigate the incident as a possible breach of PII, and he recommended that I, as I&A's IOO, defer opening a preliminary inquiry until PRIV had obtained the technical support and data it needed from HSIN in order to assess the incident for its own purposes. I followed this recommendation. I was also made aware that the I&A CIO was conducting its own inquiry that eventually resulted in the I&A AAR, and that I&A's Engagement, Liaison and Outreach (ELO) Office was collaborating with I&A CIO as well to determine which I&A products may have been improperly accessed or viewed.

On July 18, I asked the DHS Chief Privacy Officer for a status update from PRIV's privacy incident response team. My inquiry was precipitated by ILD's request for a status update to include in our quarterly report to the IOB, as the IOB would likely expect one given that the AGC/ILD had notified them of the incident on May 12. PRIV's response was that they had determined that the incident was of minimal to low impact and that no privacy notifications were required. However, it was evident to me that PRIV had not reviewed any of the *products* improperly accessed on HSIN-Intel, as they believed the only PII potentially at issue was that pertaining to HSIN account holders. In order to determine whether an IO violation had occurred, I did some initial fact gathering by asking ELO for information about the I&A products that had been improperly accessed between March 15 and May 11. ELO provided this information in a very detailed Excel spreadsheet on May 20, hyperlinked to each of the 439 I&A products at issue. I then opened an inquiry in consultation with ILD on July 26. I did not provide formal written notice to you of this inquiry, as you had long since been made aware of the incident. I verbally briefed you at a leadership management meeting that I had two relatively junior personnel on hand who could quickly review all 439 products using ELO's Excel file.

ELO's Excel spreadsheet included product names (subject of the product), the total number of improperly accessed views, the classification, the product date, if the products contained PII or USPI (according to boxes checked by the authors who posted the products), and the type of individual who improperly viewed the product (Federal User, State and Local User, Private User, and Non-US User). ELO confirmed for us that, given the type of limited "visitor" access the unauthorized HSIN users had into HSIN-Intel, they were technologically unable to download or save any of the products viewed. PIOB personnel reviewed the products and categorized them as described below, adding columns to the existing spreadsheet to include topic areas and specific issues of interest (election related, protest related, cybersecurity related,

domestic terrorism related). PIOB personnel also included secondary PII and USPER tabs to identify mismarked products.

On or around the 18th of January, I was informed of the AGC/ILD's compliance determination (refer to Section C below), which slightly modified the nature of my inquiry and necessitated that my team interview the implicated programmer in accordance with our Preliminary Inquiry SOP. On the 29th and 30th of January, the PIOB carried out interviews with both the developer responsible for the error and his federal supervisor. Both parties provided narratives consistent with the aforementioned I&A CIO AAR, attributing the incident to an attempt to rectify a permissions warning banner. The resolution of this issue was achieved by modifying the system permissions. This permission change resulted in the improper access described. The developer, who had no familiarity with HSIN, did not fully understand the implications of extending the permissions to other users. Both acknowledged the inherent challenges associated with working on systems they are not familiar with, and the trial-and-error nature of troubleshooting apparent system malfunctions.

Findings: USPI and PII

Of the 439 I&A products improperly viewed, PIOB identified 29 products containing USPI. Of these, 16 provided USPI of corporations or groups, while 13 named natural USPERs (meeting the commonly accepted definition of PII and the definition of "individual" in the Privacy Act of 1974). PIOB reviewers did not set out to additionally inventory PII on non-USPERs but anecdotally observed a small number of products that fit this category.

PIOB also identified 12 instances where products containing USPER names lacked proper PII markings. For example, in an Open-Source Intelligence Report (OSIR)(*see* attachment 2), the author correctly flagged the product for containing USPER names, but failed to mark the product as containing PII. A similar error occurred in a Joint Intelligence Bulletin (JIB)(*see* attachment 3) where the product was not flagged for PII when it contained the names of two USPERs. One OSIR (*see* attachment 4) included PII in addition to an USPER's name; specifically, it included an attachment of a social media user who posted information about a law enforcement official on a major social media platform. The publicly available social media post included the officer's name, home address, personal mobile and landline phone numbers, work address, work phone number, work fax number, badge number, and work branch. Further, the post included names, dates of birth, phone numbers, emails, and addresses of the officer's family members and girlfriend.

Findings: First Amendment Protected Activities

PIOB also identified 43 improperly accessed products that touched on potentially sensitive topics from a privacy and civil liberties perspective such as election-related topics and protest-related activities. These products did not violate the IO Guidelines but reported on potentially sensitive topics within the context of First Amendment Protected Activities.

Of the 30 election related products, 21 discussed unsuccessful foreign-based hacking attempts targeting government information technology networks associated with election

systems. The rest included miscellaneous products including field reporting highlights, newsletters, and snapshots. For example, an Online Foreign Influence Snapshot included information that Iranian state media claimed President Biden was hypocritical in critiquing Iran's human rights record and Russian state media claimed only half of Americans had high confidence that their votes would be counted accurately in the midterm election.

While some of the products did discuss protest related activities, the products focused on domestic violent extremists (DVEs) and acts of violence. An Intelligence in View (IIV) product discussed protests relating to a police training facility in Atlanta. The piece highlighted media praising actions like throwing stones, fireworks, and Molotov cocktails at police.

Other general observations

- The 439 I&A products on HSIN-Intel were improperly accessed a total of 1,525 times.
- Of the unauthorized views, 437 were federal users, 524 were state and local users, 518 were private sector users, and 46 were non-U.S. citizens. Federal, state and local viewers encompassed 63% of total views followed by private users encompassing 34% of views.
- HSIN-Intel is restricted to government users only, but according to ELO, most of the HSIN users who were federal, state or local government officials and gained access to HSIN-Intel through the coding error were eligible to request and be considered for access to HSIN-Intel had they gone through the formal request/approval process. Thus, the 437 federal and 524 state and local HSIN users were potentially authorized recipients of I&A intelligence.
- Many of the HSIN users who were non-U.S.-based or nongovernmental may also be authorized recipients of I&A intelligence. They simply weren't eligible to access the intelligence via HSIN-Intel, but could have accessied it via other HSIN platforms, such as HSIN- Critical Infrastructure which allows non-U.S.-based and nongovernmental partners to access the system.
- The non-U.S. citizens viewed 46 products, almost entirely concerning cyber security.
- Over 169 improperly accessed HSIN-Intel products involved cybersecurity, making up 39% of all products. These products involved malicious cyber activity by foreign-based internet protocol addresses and domains, advanced persistent threat actors, and unsuccessful foreign-based connection attempts targeting government information technology.

C. Compliance Determination

Upon the advice of the AGC/ILD, I have concluded that the dissemination of intelligence products via HSIN-Intel constitutes an intelligence activity subject to the IO Guidelines. As noted above, 29 of the 439 products inadvertently made accessible to unauthorized HSIN users contained USPI. Although unintentional, these disseminations fell short of the requirement of Section 2.3 of the IO Guidelines that dissemination be reasonably believed to further one or more of I&A's national or departmental missions, and, in the case of intelligence containing USPI, the

requirement of Section 2.3.1 that I&A reasonably believe the dissemination will advance one or more of the recipients' lawful intelligence, counterterrorism, law enforcement, or other homeland security-related functions. As a result, the I&A contract developer's March 15 coding error that resulted in the inadvertent dissemination of HSIN-Intel's library of intelligence products to recipients without first making the determinations required by Sections 2.3 and 2.3.1 constituted a violation of I&A's IO Guidelines.

D. Attestation

Through my electronic signature below, I attest that the report above reflects my factual findings and compliance determination regarding Compliance Inquiry No. 2023-03.

(b) (6)

(b) (6), (b) (7)(C)
Intelligence Oversight Officer
Office of Intelligence and Analysis
U.S. Department of Homeland Security