# FISA Query Audit

## Office of Internal Auditing (OIA)

May 10, 2023

# Agenda

| Agenda Topics | Slide # |
|---|---|
| Query Audit 1 (QA1) Testing Summary | 3 |
| Enhancements Implemented by the FBI between QA1 and QA2 | 4 |
| Query Audit 2 (QA2) Testing Summary | 5 |
| Compliance Results | 6 |
| Audit Observations and Associated Recommendations | 7 |
| *Appendix: Risk-Based Sampling Summary* | 8 |

# Query Audit 1 (QA1) Testing Summary

**Objective:** In May 2021, OIA began to execute the FBI's first enterprise-wide internal audit of queries of unminimized "raw" FISA-acquired information. OIA selected the twelve (12) month audit period of April 1, 2020 through March 31, 2021 to independently assess queries against raw FISA against the query standard. This audit resulted in baseline compliance metrics to compare against for future query audits.

## Planning

- Obtained [redacted] and [redacted] FISA query logs for the audit period of April 1, 2020 through March 31, 2021 from ITADD.

## Sampling[1]

- Selected 2,159[3] queries of both traditional FISA and Section 702 acquired information based on a perceived level of risk.

## Execution

- Tested all 2,159 FISA queries for compliance with the query standard.[2]
- Evaluated a subset of 1,385 queries that also searched raw FISA Section 702 collection to determine whether users properly identified queries containing a United States person (USPER) or presumed USPER term.

## Adjudication

- In coordination with Department of Justice (DOJ) - Office of Intelligence (OI), OIA made preliminary compliance determinations based on the query standard.
- The results of the first enterprise-wide internal audit were leveraged to establish a baseline compliance for future audits.

[1] OIA leveraged the following authoritative guidance pertaining to sampling: AICPA §530 – Audit Sampling (2021), U.S. Government Accountability Office (GAO) Government Auditing Standards, and consultation with Sampling Specialists to arrive at this sample size.
[2] As noted within the *FBI FISA Query Guidance (November 2021): "The FBI FISA querying standard has the following three components… A query must: (U) Have an authorized purpose: the person conducting the query must have the purpose of retrieving foreign intelligence information or evidence of a crime from raw FISA collection; (U) Be reasonably designed: the query term must be reasonably tailored to retrieve foreign intelligence information or evidence of a crime without unnecessarily retrieving other information from raw FISA collection; and (U) Be justified: the person conducting the query must have a specific factual basis to believe that the query is reasonably likely to retrieve foreign intelligence information or evidence of a crime from raw FISA collection."*
[3] As noted within the Compliance Results slide, OIA determined 1,776 (82%) of these 2,159 queries were compliant with the query standard.

# Enhancements Implemented by the FBI between QA1 and QA2

The FBI instituted the following internal controls and system changes to enhance compliance.

## Opt In/Opt Out

[redacted] data sets, including raw FISA data, were excluded from searches by default. Within [redacted], raw Section 702 collection was excluded from searches by default. These updated system defaults require the user to opt-in to raw FISA/702 data sets.

## Batch Job Approval

The Deputy Director communicated to all FBI personnel via email that users are required to obtain attorney approval prior to executing a [redacted] batch job of 100 or more queries against raw FISA data sets (except where exigent circumstances exist).

## New Query Training

The FBI launched new and enhanced FISA query training on Virtual Academy (VA), the internal training platform utilized by the FBI.

## System Integration

The FBI integrated [redacted] with VA, for the majority of mandatory query trainings, to mitigate the risk of users obtaining access to raw FISA without completing the required trainings.

# Query Audit 2 (QA2) Testing Summary

**Objective:** In August 2022, OIA sought to evaluate whether FBI management's changes had the expected positive impact on the FBI's querying compliance. OIA selected the nine (9) month audit period of July 1, 2021 through March 31, 2022 to measure the impact of the internal controls and system changes as noted on the preceding slide.

## Planning

- Obtained [redacted] and [redacted] FISA query logs for the audit period of July 1, 2021 through March 31, 2022 from ITADD.
- Ingested logs into our data analytics Query Navigator (PowerBI) tool, allowing us to quickly process the files, perform data integrity checks, and sample queries for testing.

## Sampling

- Selected 227 queries that users marked as "evidence of a crime only" for purposes of testing, based on perceived risk.[1]
- Selected an additional 331 queries for testing,[2] bringing the full QA2 sample total to 558 queries.

## Execution

- Deployed SharePoint survey to the selected queries' 343 respective users; questions included asking the user to articulate how their query met the query standard.
- Tested all 558 FISA queries for compliance with the query standard.[3]
- Evaluated a subset of 446 queries that also searched raw FISA Section 702 collection to determine whether users properly identified queries containing a United States person (USPER) or presumed USPER term.

## Adjudication

- Shared preliminary compliance determinations based on OIA's understanding of the query standard with DOJ-OI.
- Updated OIA's reported compliance determinations to reflect DOJ-OI's compliance determinations.

[1] In conjunction with our adjudication process, OIA determined 218 (96%) of these 227 queries were compliant with the query standard. As later noted in our observations, OIA has found that users are confused by the term "evidence of a crime only" and routinely select that option mistakenly.

[2] OIA leveraged the following authoritative guidance pertaining to sampling: AICPA §530 – Audit Sampling (2021), U.S. Government Accountability Office (GAO) Government Auditing Standards, and consultation with Sampling Specialists to arrive at this sample size. OIA leveraged statistician-provided sample tables (using an 25% error rate, 95% confidence level, 5% margin of error) to arrive at this sample size.

[3] As noted within the *FBI FISA Query Guidance (November 2021): "The FBI FISA querying standard has the following three components… A query must: (U) Have an authorized purpose: the person conducting the query must have the purpose of retrieving foreign intelligence information or evidence of a crime from raw FISA collection; (U) Be reasonably designed: the query term must be reasonably tailored to retrieve foreign intelligence information or evidence of a crime without unnecessarily retrieving other information from raw FISA collection; and (U) Be justified: the person conducting the query must have a specific factual basis to believe that the query is reasonably likely to retrieve foreign intelligence information or evidence of a crime from raw FISA collection."*

# Compliance Results

## QUERY STANDARD

FISA queries must have an authorized purpose, be reasonably designed, and be justified. "Justified" means the person conducting the query must have a *specific factual basis* to believe that the query is reasonably likely to retrieve foreign intelligence information or evidence of a crime from raw FISA collection. Below are the results of our testing of queries of raw traditional FISA collection[1] for compliance with the query standard.

| | Query Audit 1 | | Query Audit 2 | |
|---|---|---|---|---|
| **Compliant** | **1,776** | *82%* | **518** | *96%* |
| **Non-Compliant** | | | | |
| • **Insufficient justification** | 359 | *17%* | 17 | *3%* |
| • **Unreasonably designed** | 16 | *1%* | 3 | *1%* |
| • **Lack of authorized purpose** | 8[2] | *0%* | 0 | *0%* |
| **Total Non-Compliant Queries** | **383** | *18%* | **20** | *4%* |
| **Queries Tested** | **2,159** | *100%* | **538**[3] | *100%* |

**Insufficient Justification[4] (17)**

- (8) looking for connections in raw FISA collection;
- (2) January 6th Capitol violence;
- (2) processing open Guardians;
- (1) Afghan refugee vetting;
- (1) domestic terrorism matters;
- (1) per request from an OGA or FBI LEGAT;
- (1) CHS vetting / recruitment efforts;
- (1) typographical error (phone number with omitted digit).

## USPER LABELING

For queries run against raw FISA Section 702 collection, users must properly identify and record when the query contains an USPER or presumed USPER query term.

| | Query Audit 1 | | Query Audit 2 | |
|---|---|---|---|---|
| ***Section 702*** **Queries Tested** | **1,385** | *100%* | **446** | *100%* |
| **USPERs Marked as Non-USPER** | 59 | *4%* | 8 | *2%* |

[1] Note that of the 558 queries selected for testing, 446 (80%) of these queries searched against raw Section 702 collection in addition to searching raw traditional FISA collection. Of these 446 queries of raw Section 702, users marked 286 of the query terms (64%) as USPER or presumed USPER and 160 of the query terms (36%) as non-USPERs.

[2] Seven (7) of these queries were performed in [redacted] and [redacted] during informal training (e.g., individuals showing fellow colleagues how to query FISA) and formal training (e.g., Basic Training Courses). While there are training exceptions to the query standard articulated within the FBI's Section *702 Query Procedures,* based on OIA's evaluation of each query's facts and circumstances, OIA, in collaboration with the FBI Office of the General Counsel (OGC)-National Security and Cyber Law Branch (NSCLB), determined these queries did *not* meet those exceptions primarily because the users queried USPER terms without a "particular need" to do so. The one (1) remaining query related to a user improperly querying the full name of the victim of a crime to assist the victim in locating their misplaced Internet Crime Complaint Number.

[3] As noted within the Testing Approach slide, our initial QA2 sample consisted of 558. There were 20 queries for which both OIA and DOJ-OI, for various reasons, were not able to determine the query's compliance with the query standard. Note, DOJ-OI is planning to report these queries to the FISC in a Rule 13(b) notice stating that DOJ-OI is *"unable to reach a determination…due to an inability to gather additional information."*

[4] One of OIA's recommendations for FBI management's consideration is that the FBI require users to contemporaneously document in the system their query's justification when the user is executing a FISA query. This requirement will force users to evaluate their query's compliance with the query standard before executing a query. OIA believes this can prevent many (what would be) non-compliant queries from being run in the system.

# Audit Observations and Associated Recommendations

Informed by our audit procedures performed, the following chart summarizes the observations from the FBI's audit of FISA querying procedures. For each observation, OIA has worked with stakeholders and executive management to develop recommendations designed to prevent and detect further non-compliant queries.

| Audit Observations | OIA Recommendations |
|---|---|
| 1) The FBI does not require users to document how the query meets the justification standard at the time the query is executed. | • Evaluate the feasibility and operational impact of recording the justification at the time the query is performed. |
| 2) The FBI's current FISA query compliance monitoring program requires enhancements. | • Develop a more robust FISA query compliance monitoring process.<br>• Build data analytics solutions to allow for monitoring queries on a near real-time basis. |
| 3) OIA identified issues with the implementation and monitoring of the batch job attorney approval control. | • Re-evaluate the batch job attorney approval control for design improvements and continue to assess the operating effectiveness of the control. |
| 4) During the audit period, there were instances of users performing queries against unminimized FISA-acquired information without completion of all required trainings. | • Complete the implementation of system control enhancements to ensure users complete all mandatory training requirements prior to gaining access to systems containing raw FISA information. |
| 5) OIA identified instances where users were not clear on how to practically apply the query standard. | • Enhance existing training to integrate users' understanding of the system functionality with the underlying legal requirements.<br>• Periodically update existing training to explicitly address known compliance incidents.<br>• Enhance guidance and prompts in FISA query system user interfaces to promote compliant queries. |
| 6) The audit identified instances where users were confused by the term "evidence of a crime only" and selected that option mistakenly, which led to further inaccurate selections in the system. | • Implement a system change to clarify options for the user that highlights the limited and infrequent circumstances in which a user should select "evidence of a crime only". |
| 7) OIA identified users incorrectly using product IDs and FBI case file numbers as query terms and then mislabeling the USPER status of the query term. | • Notify all users who performed non-compliant queries of this nature and provide guidance and remedial training to help them correctly use the system features in a compliant manner.<br>• Evaluate potential system controls to guide compliant user behavior. |

# Appendix: Risk-Based Sampling Summary

1) OIA leveraged the following authoritative guidance pertaining to sampling: AICPA §530 – Audit Sampling (2021), U.S. Government Accountability Office (GAO) Government Auditing Standards, and consultation with Sampling Specialists and certified statisticians to determine the minimum acceptable sample size for an audit of this nature.

2) Using a risk-based and judgmental sampling approach, OIA analyzed a population of queries in order to select samples for substantive and control testing (i.e., dual-purpose testing) for QA1 and QA2.

3) To minimize sampling risk, the methodology utilized by OIA ensures that all queries performed in the audit period were subject to sampling.

*The auditor might first separately examine those items deemed to be of relatively high risk and then use audit sampling (which will involve some form of probabilistic selection) to form an estimate of some characteristic of the remaining population.*
*- AICPA §530 – Audit Sampling (2021)*

*"The sample size can be determined by the application of a statistically based formula or through the exercise of professional judgment."*
*- AICPA §530 – Audit Sampling (2021)*