



Audit of the Federal Bureau of Investigation's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance



AUDIT DIVISION

25-065

June 2025

REDACTED FOR PUBLIC RELEASE

The full version of this report contains classified information that if released publicly could compromise national security interests and the FBI's operations. To create this public version of the report, the Office of the Inspector General redacted (blacked out) portions of the full report.



(U) EXECUTIVE SUMMARY

(U) Audit of the Federal Bureau of Investigation's Efforts to Mitigate the Effects of Ubiquitous Technology

(U) Objectives

(U) Our audit objectives were to determine the sufficiency and effectiveness of the: (1) actions the Federal Bureau of Investigation (FBI) is taking to protect sensitive investigations and operations from technological compromise and whether those steps have been taken at the enterprise level, and (2) training the FBI provides to its personnel to increase the work force's resiliency against technological compromise.

(U) Results in Brief

(U) Since the issuance of our Management Advisory Memorandum (MAM) to the FBI Director in December 2022, which identified immediate concerns regarding the FBI's management of the Ubiquitous Technical Surveillance (UTS) threat, the FBI has taken several positive actions. These actions included elevating the threat to a "Tier 1" enterprise risk and forming a "Red Team" to address the threat FBI-wide. However, we do not believe that the initial effort of the Red Team to identify the specific, enterprise-wide risks was adequate, potentially leaving several UTS-related threats unmitigated. We are particularly concerned that the Red Team's recent threat mitigation efforts did not adequately consider existing FBI efforts to mitigate the UTS threat, and that it did not include a sufficient long-term vision for how the FBI will approach the evolving UTS threat after its initial action items are addressed. In addition, the FBI continues to develop a UTS Strategic Plan, which we believe is needed; however, after reviewing an initial outline for the plan, we are concerned that the final version may not be sufficient to ensure that responsibilities are clearly assigned to officials who have the authority to execute the strategy and ensure that the FBI has clear and unambiguous UTS-related policies throughout the enterprise. We are also concerned that the forthcoming strategy will not adequately create clear lines of authority when the FBI must respond to UTS-related security incidents.

(U) Recommendations

(U) Our report makes four recommendations to improve how the FBI responds to the evolving UTS threat. The FBI's official response is in Appendix 8. The FBI neither concurred nor disagreed with our recommendations but stated it would take

corrective actions to address our recommendations. Appendix 9 details actions necessary to close the recommendations.

(U) Audit Results

(U) The FBI defines UTS as the widespread collection of data and application of analytic methodologies for the purpose of connecting people to things, events, or locations. Although the risks posed by UTS to the FBI's criminal and national security operations have been longstanding, recent advances in commercially available technologies have made it easier than ever for less-sophisticated nations and criminal enterprises to identify and exploit vulnerabilities created by UTS. Some within the FBI and partner agencies, such as the Central Intelligence Agency (CIA), have described this threat as "existential."

(U) Because of the significance of this ever-evolving threat, in December 2022, the Office of Inspector General (OIG) issued a MAM to the FBI Director highlighting two immediate issues that needed to be addressed: 1) the FBI's response to the UTS threat was disjointed and inconsistent, and 2) training efforts across the FBI needed to be improved.

(U) Enterprise Risk and Internal UTS Threat Assessment

(U) In response to the first issue highlighted in our MAM, the FBI Director elevated the UTS threat to a "Tier 1 Enterprise Risk" and instructed the FBI's Office of Integrity and Compliance (OIC) to conduct an internal review of the threat. In January 2023, OIC established a "Red Team" comprised of senior executives from each FBI division. The goals of the Red Team were to: (1) identify vulnerabilities, (2) develop a plan to mitigate those vulnerabilities, and (3) present a report to the Director detailing that mitigation plan.

(U) Efforts to Identify UTS Vulnerabilities Were Inadequate and Mitigation Plan Lacked Long-Term Vision

~~(S//NF)~~ The first primary goal of the OIC-led Red Team was to identify vulnerabilities in each FBI division and develop a "gap analysis" which would serve as the foundation for the second goal to develop a mitigation plan. When we requested documentation of the gap analysis performed by the FBI, we were provided [REDACTED]

[REDACTED] generalized vulnerabilities in the areas of policy, [REDACTED] and training. (See Exhibit 1 in the body of this report). In reviewing this document, we noted that it did not appear to account for known UTS vulnerabilities already identified by the FBI. Specifically, prior to the creation of the Red Team, and at the request of the Assistant Director of the Counterintelligence Division (CD) at the time, CD conducted its own independent review of how UTS [REDACTED]. This review identified over [REDACTED] vulnerabilities throughout the FBI in [REDACTED]. Although CD presented the results of its findings to the Red Team, we were not provided with evidence that the Red Team incorporated or even considered many of the specific vulnerabilities identified in CD's analysis. In fact, we were told during the audit that the Red Team opted to keep its gap analysis at a higher level with an emphasis on generalized UTS policy, [REDACTED], and training gaps.

(U) We believe the large number of vulnerabilities identified in CD's analysis clearly evidences that the universe of FBI vulnerabilities is far greater than what was captured in the Red Team's gap analysis. Further, the Red Team's decision to keep the gap analysis at such a high level, without documenting that the vulnerabilities previously identified by CD were appropriately considered, may have significantly impacted the comprehensiveness of the resulting draft mitigation plan. Notably, after the FBI reviewed a draft of this report, it informed us that the document titled "UTS Red Team Gap Analysis" was only intended to be an "outline" for the gap analysis. According to the FBI, it is now in the process of creating a "crosswalk" to document how each of the vulnerabilities from CD's analysis were actually considered in the Red Team's gap analysis and resulting draft mitigation plan. We think the creation of this "crosswalk" is a worthwhile exercise to confirm whether the universe of vulnerabilities identified in CD's analysis are addressed in the mitigation plan.

(S//NF) In September 2023, we reviewed the FBI's draft mitigation plan, which remains under review by FBI executive management. The draft mitigation plan that we reviewed included [REDACTED] items after the FBI's review of a draft version of this report) organized into 6 categories: Policy; Procedures and Analysis; Training; [REDACTED]; Monitoring; and Auditing and Inspections. Due to the lack of a well-documented gap analysis, it was unclear whether all vulnerabilities were identified and which identified vulnerabilities each of the mitigation plan's action items were designed to address.

(S//NF) Further, many of the [REDACTED] items appeared to be short-term in nature, with some already marked as "complete" in the draft plan. When we asked the FBI if it had developed a longer-term approach to ensure its focus remained on the evolving UTS threat after the [REDACTED] items were closed and

the work of the Red Team was finished, we were told that the "Monitoring" and "Auditing and Inspections" categories were intended to address the longer-term UTS strategy. In our opinion, these areas of the draft plan do not provide a sufficiently clear, actionable long-term approach to address the UTS threat or ensure all future UTS initiatives and UTS-related incidents are addressed in a manner consistent with federal law and FBI policy.

(U) Future UTS Strategic Plan Must Be Comprehensive

(S//NF) After we raised concerns about the long-term approach for the FBI's UTS efforts, we were informed that the FBI Directorate of Intelligence (DI) began developing an FBI-wide UTS Strategic Plan designed to specifically address both this concern and our MAM recommendation related to FBI's disjointed and inconsistent UTS efforts. According to DI, the forthcoming UTS Strategic Plan will [REDACTED] and will sync with the FBI's five-year intelligence program strategy. We reviewed a draft outline of the UTS Strategic Plan. Although the outline recognizes the need to execute an enterprise-level approach to the UTS threat and to "create an organizational framework with authorities to address UTS," it does not appear to address the need to assign responsibilities to officials with the authority to execute the strategy or a clear line of authority for responding to UTS-related incidents. Additionally, based on the outline, we are concerned that the Strategic Plan will not adequately address how to best leverage the disparate FBI entities with UTS expertise to benefit the entire enterprise.

(S//NF) Data Breach Exposes [REDACTED] the FBI's Policies and Procedures for How to Respond to Such a Breach

(S//NF) In [REDACTED] we were made aware of a data breach [REDACTED]. The FBI did not have policies or procedures in place [REDACTED].

(U) Expansion of UTS Training

(U) In response to the OIG MAM, we found that the FBI took steps to update and expand the UTS training available to its employees. However, many of the advanced UTS courses remain optional and are unable to serve many students due to resource constraints. Accordingly, we remain concerned that many agents are not attending these important courses [REDACTED] and we believe that the FBI must take additional steps to ensure all personnel at all levels are adequately trained on the skills they need to respond to the UTS threat.

Table of Contents

(U) Introduction.....	1
(U) Examples of the UTS Threat.....	1
(U) OIG Audit Approach	2
(U) OIG Management Advisory Memorandum	3
(U) Audit Results	4
(U) Enterprise Risk and Internal UTS Threat Assessment	4
(U) Examples of FBI Efforts to Protect Investigations, Operations, and Personnel Prior to 2023	4
(U) UTS as a Tier 1 Enterprise Risk and Red Team Efforts in 2023	5
(U) Red Team “Gap Analysis”	5
(U) Counterintelligence Division’s Anatomy of a Case	8
(U) Red Team Draft Mitigation Plan.....	9
(U) Development of the FBI’s New UTS Strategic Plan.....	11
(S//NF) Data Breach Exposes [REDACTED] Gaps in the FBI’s Policies and Procedures for How to Respond to Such a Breach	12
(U) UTS-Related Training Efforts.....	13
(U) Conclusion and Recommendations	14
(U) APPENDIX 1: Objectives, Scope, and Methodology.....	15
(U) Objectives	15
(U) Scope and Methodology	15
(U) Statement on Compliance with Generally Accepted Government Auditing Standards.....	15
(U) Internal Controls	15
(U) Compliance with Laws and Regulations.....	16
(U) Computer-Processed Data	16
(U) APPENDIX 2: Examples of the UTS Threat.....	17
(U) Examples of UTS Risks	17
(U) Visual and Physical Imagery.....	17
(U) Use of FBI Affiliated Electronic Communications	17
(U) Financial Transactions.....	17
(U) Travel Data Correlation	17
(U) Online Presence and Electronic Communications.....	18
(U//FOUO) [REDACTED]	18
(U//FOUO) [REDACTED]	18

(U) Combination of Vulnerabilities 18

(U) APPENDIX 3: Lessons Learned by Other Government Agencies 20

(U) Central Intelligence Agency 20

(U) Defense Intelligence Agency 21

(U) APPENDIX 4: FBI’s Decentralized Attempts to Address UTS 22

(U) Counterterrorism Division’s Advanced Projects Unit 22

(U) International Operations Division’s Strategic Intelligence Unit 22

(U//FOUO) [REDACTED] 22

(U) New York Field Office 22

(U) Washington Field Office 22

(U) APPENDIX 5: Management Advisory Memorandum 23-013 23

(U) APPENDIX 6: CD’s Anatomy of a Case 32

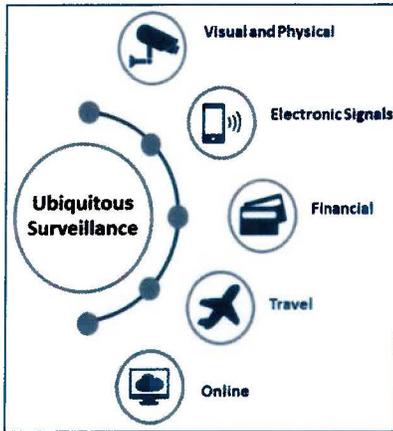
(U) APPENDIX 7: Acronyms 35

(U) APPENDIX 8: The Federal Bureau of Investigation’s Response to the Draft Audit Report 36

(U) APPENDIX 9: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Audit Report 41

(U) Introduction

(U) The Federal Bureau of Investigation (FBI) defines Ubiquitous Technical Surveillance (UTS) as the widespread collection of data and application of analytic methodologies for the purpose of connecting people to things,



events, or locations.¹ This data is categorized in five vectors: (1) Visual and Physical – identification of people or objects tied to an operation through cameras or physical surveillance; (2) Electronic Signals – use of electronic devices such as mobile phones; (3) Financial – transactional financial records with unique identifiers linked to a specific account holder; (4) Travel – records that include unique identifiers for hotel stays, border crossings, plane reservations, etc. (5) Online – advertising data from web browsing and social media use, etc.

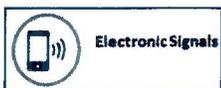
(S//OC/NF) The potential impacts of UTS technologies on the operations of a federal agency are substantial. [REDACTED]

(S//NF) As the nation's lead domestic agency for national security-related investigations, the FBI currently faces risks [REDACTED]

[REDACTED] are currently being used against its employees, assets, and operations.³ The FBI is aware of prior and ongoing UTS compromises that have impacted FBI operations, threatened the safety of its sources, and are currently being used by adversaries to challenge the United States Government on a global scale. Some within the FBI and partner agencies like the CIA have described the threat as "existential."

(U) Examples of the UTS Threat⁴

(U) As noted above, the threat of UTS is not new. In recent years, the FBI has grappled with UTS compromises in each of the five vectors. The following few examples help illustrate the significance of this pervasive threat, the corresponding consequences of poor tradecraft, and the potential repercussions of not having a clear strategy to address the threat.



(S//NF) [REDACTED]

¹ (U) This definition comes from the UTS briefing provided by the FBI Counterintelligence Division as of the time of this audit.

² (U//FOUO) [REDACTED]

³ (S//NF) [REDACTED]

[REDACTED] this report focuses on the FBI's efforts to protect its personnel and operations from the UTS threat (defensive techniques).

⁴ (U) Additional illustrative examples of the UTS threat can be found in Appendix 2.

[REDACTED]



(S//NF)

[REDACTED]



(U) In 2018, while the FBI was working on the "El Chapo" drug cartel case, an individual connected to the cartel contacted an FBI case agent. This individual said that the cartel had hired a "hacker" who offered a menu of services related to exploiting mobile phones and other electronic devices. According to the individual, the hacker had observed people going in and out of the United States Embassy in Mexico City and identified "people of interest" for the cartel, including the FBI Assistant Legal Attaché (ALAT), and then was able to use the ALAT's mobile phone number to obtain calls made and received, as well as geolocation data, associated with the ALAT's phone. According to the FBI, the hacker also used Mexico City's camera system to follow the ALAT through the city and identify people the ALAT met with. According to the case agent, the cartel used that information to intimidate and, in some instances, kill potential sources or cooperating witnesses.



(S//NF)

[REDACTED]

(U) OIG Audit Approach

(U) Our preliminary objectives were to determine the sufficiency and effectiveness of the: (1) actions the FBI is taking to protect sensitive investigations and operations from technological compromise and whether those steps have been taken at the enterprise level, and (2) training the FBI provides to its personnel to increase its work force's resiliency against technological compromise. To accomplish our objectives, we reviewed FBI policy and guidance related to tradecraft, including the FBI's Confidential Human Source Policy Guide and the Domestic Investigations and Operations Guide. In addition, we interviewed 79 FBI officials, including personnel from 7 FBI field offices – Chicago, Illinois; Columbia, South Carolina; Houston, Texas; New York, New York; Philadelphia, Pennsylvania; Richmond, Virginia; and Washington, D.C. – as well as individuals from FBI Headquarters, Redstone Arsenal in Huntsville, Alabama, and both the Training Division and Laboratory Division in Quantico, Virginia. We also interviewed personnel from CIA and the Defense Intelligence Agency about tradecraft issues.

(U) Appendix 1 contains additional information on our audit objectives, scope, and methodology.

(U) **OIG Management Advisory Memorandum**

(U) Because of the significance of this ever-evolving threat, as part of this audit in December 2022, the OIG issued a Management Advisory Memorandum (MAM) to the FBI Director which highlighted two immediate issues that needed to be addressed as we continued our work on this audit: 1) the FBI's response to the UTS threat was disjointed and inconsistent, and 2) efforts to train personnel across the FBI needed to be improved. Throughout the Audit Results section below, we described the steps the FBI took in response to the MAM and areas where we believe additional improvements are required.⁵

⁵ (U) A complete copy of the MAM, including the FBI's response to the draft, and the OIG's summary of actions needed to close the recommendations can be found in Appendix 5.

(U) Audit Results

(U) Although the FBI took several positive steps to address the concerns we raised in our December 2022 Management Advisory Memorandum (MAM) related to its disjointed approach to the Ubiquitous Technical Surveillance (UTS) threat, we believe more should be done. Specifically, the FBI's decision to elevate the UTS threat to a Tier 1 enterprise risk and to form a "Red Team" to address the threat FBI-wide were major strides toward dealing with the problem on an enterprise-level. However, we are concerned that the Red Team's initial efforts to identify the specific UTS vulnerabilities across the enterprise and its resulting draft mitigation plan were not comprehensive, potentially leaving many UTS vulnerabilities unaddressed. We also found that despite the Red Team's efforts and a recent, ongoing initiative led by the Directorate of Intelligence (DI) to develop a UTS Strategic Plan, the risk of existing UTS efforts remaining disjointed and uncoordinated still exists because the forthcoming Strategic Plan does not appear to assign responsibilities to officials with the authority to execute the strategy and ensure that the FBI has clear and unambiguous UTS-related policies throughout the enterprise. In addition, the forthcoming plan does not appear to address the need for a clear line of authority for responding to UTS-related incidents, nor does it address how the disparate entities within the FBI with UTS expertise will coordinate to avoid duplication of UTS efforts and scale UTS initiatives to benefit the entire enterprise. Finally, although the FBI updated and expanded the basic UTS training provided to FBI personnel, we do not believe the more advanced UTS training is reaching enough of the personnel who require such training.

(U) Enterprise Risk and Internal UTS Threat Assessment

(S//NF) As noted above, officials from both the FBI and the CIA described the threats posed by UTS as "existential" to the way the FBI does business. These officials agreed that, if not adequately addressed, UTS can lead to unacceptable outcomes such as: [REDACTED]; significant national security and criminal operations and investigations being compromised; [REDACTED]

(U) The FBI had made efforts to address the UTS threat prior to the issuance of our MAM in December 2022 and continues to do so today. However, we are concerned that some of these recent efforts have been inadequate and may not fully leverage existing resources and prior UTS-related initiatives within various components of the FBI.

(U) Examples of FBI Efforts to Protect Investigations, Operations, and Personnel Prior to 2023

(S//NF) As we described in our MAM, the FBI had previously undertaken several initiatives to protect itself from the UTS threat. However, those efforts to protect its personnel, investigations, operations, and sources were generally disjointed and uncoordinated. [REDACTED]

[REDACTED], the FBI created several working groups focused on the UTS threat led by Section Chiefs from the operational divisions. This initiative ultimately led to the creation of the Operational Security and Tradecraft Unit (OSTU) within the FBI's DI. OSTU was initially intended to provide enterprise-wide tradecraft education and eventually become an office supporting the entire FBI, incorporating OSTU and the Human Intelligence (HUMINT) Operations Training Unit from DI, as well as the Covert Backstopping Unit from the Criminal Investigative Division's National Covert Operations Section. [REDACTED]

[REDACTED] However, for a multitude of reasons which included, but were not limited to, resource issues and turnover of key leadership positions, the proposal to elevate OSTU into the "Office of Tradecraft" never materialized even though DI officials

described OSTU to us as a possible avenue to address the UTS threat across the enterprise. As a result, and despite its expertise in addressing UTS threats and its ongoing communication with IC partners about UTS best practices, OSTU currently has no authority to compel FBI personnel to operationalize those best practices or take any particular actions to mitigate UTS threats to FBI operations.

(S//NF)



(U) UTS as a Tier 1 Enterprise Risk and Red Team Efforts in 2023

(U) As a result of our first MAM recommendation, in January 2023 former Director Wray established UTS as a "Tier 1 Enterprise Risk" and instructed the FBI's Office of Integrity and Compliance (OIC) to conduct an internal review of the UTS threat. In response, OIC established a "Red Team" of Senior Executive Service personnel from each division to address the threat posed by UTS. The primary goals of the Red Team were threefold: (1) identify vulnerabilities within each division, (2) develop a plan to mitigate those vulnerabilities, and (3) present a report to the Director detailing that mitigation plan.

(U) The Red Team officially kicked off its efforts on January 19, 2023, with an introduction and brief overview by the Executive Assistant Director of the Intelligence Branch and the Assistant Director of OIC. Twenty-two FBI officials, including 13 SES-level officials (representing 11 divisions) attended the initial introductory meeting. The first working meeting, which was held shortly thereafter on February 2, 2023, led to the creation of a roster of approximately 30 Red Team members. The roster included OIC officials that would facilitate the Red Team, SES level representatives from 22 divisions, as well as other subject matter experts. In addition, there were approximately 10 subject matter experts and senior officials that were regularly kept apprised of the Red Team's work and occasionally attended the subsequent meetings.

(U) Red Team "Gap Analysis"

(U//FOUO) As part of its goal to identify the UTS vulnerabilities in each FBI division, the Red Team conducted a "gap analysis" across the divisions to serve as the foundation of its goal to develop a mitigation plan for the Director's review. Each participating FBI division was responsible for conducting an internal gap analysis and assigning the identified gaps to the following six categories: (1) Policy, (2) Procedures, (3) Training, (4) , (5) Monitoring, and (6) Auditing.

⁶ (U) Five Eyes is an intelligence sharing partnership which includes Australia, Canada, New Zealand, the United Kingdom, and the United States.

(S//NF) When we asked for documentation of the gap analysis that was performed, we were provided with a document titled "UTS Red Team Gap Analysis." (See Exhibit 1), This document, provided to us in January 2024, was a single-page of high-level, generalized vulnerabilities in only three of the above six categories - Policy, [REDACTED], and Training. Procedures, Monitoring, and Auditing were unaddressed in the document, but found in the mitigation plan described below. For the three categories that were included, the document contained no details, explanations, or analysis. For example, the Policy section only noted that the FBI's Confidential Human Source Policy Guide was updated [REDACTED] related to policy. In the [REDACTED] section of the Gap Analysis, it noted that [REDACTED]

The Red Team identified

(U) Exhibit 1

(U) Documentation of the Red Team's Gap Analysis

~~SECRET//NOFORN~~

UTS RED TEAM GAP ANALYSIS

1) Are the policies that we currently have sufficient?

2) What enhancements do we need to do?

3) Are the trainings that we currently have sufficient?

~~Classified By:~~
~~Derived From: FBI NSICG~~
~~Declassify On: 50Y1-UM~~

~~SECRET//NOFORN~~
FBI DOJ - OIG UBIQUITOUS TECHNOLOGY - 000104

(U) Source: FBI

(U//FOUO) In addition, the document provided to us did not address potential resource gaps as noted in our December 2022 MAM. MAM 23-013, recommendation 1 asked the FBI to [REDACTED] [of an FBI-wide approach to mitigating each of the threats identified]."⁷

(U) *Counterintelligence Division's Anatomy of a Case*

(S//NF) The Red Team's analysis of the UTS threat was considerably less detailed than at least one prior effort to document similar threats facing the FBI. Prior to the establishment of the Red Team, the Counterintelligence Division (CD) conducted an extensive, independent review of how UTS risks could affect a typical FBI investigation, which it called *Anatomy of a Case*. This assessment was developed at the request of the Assistant Director of CD, and its goal was to identify the areas of any FBI case (not just CD cases) that are vulnerable to threats posed by UTS and illustrate the wide range of risks posed to the FBI's work by UTS. *Anatomy of a Case* [REDACTED]

(U) After *Anatomy of a Case* was completed, its distribution was limited due to the sensitivity of its subject matter. In fact, when we spoke to OIC in February 2023 and asked if the document could potentially serve as a blueprint for the Red Team's mission of identifying UTS vulnerabilities, OIC told us that it was not aware of the effort. Based on our inquiry, in an early March 2023 meeting CD presented *Anatomy of a Case* to the Red Team for its consideration. According to minutes from the next meeting, members appeared to be unsure whether to identify specific vulnerabilities as *Anatomy of a Case* had done or look at broader gaps across the enterprise. The Directorate of Intelligence (DI) suggested each division focus on broader policy and training gaps related to UTS rather than specific vulnerabilities. Ultimately, the Red Team's Gap Analysis did not appear to account for most of the vulnerabilities that CD had identified.

(S//NF) We believe the [REDACTED] vulnerabilities identified in CD's *Anatomy of a Case* clearly demonstrated that the universe of FBI vulnerabilities is far greater than what appeared to be captured in the Red Team's gap analysis. For example, CD's analysis specifically identified [REDACTED]

[REDACTED] Accordingly, we believe the Red Team's decision to keep its gap analysis at such a high-level without explicitly accounting for and documenting known, specific vulnerabilities already identified within the FBI may have significantly impacted the comprehensiveness of the resulting mitigation plan, potentially leaving many UTS threats unaddressed throughout the FBI. We describe our concerns with the resulting draft mitigation plan below.

(U) After reviewing a draft version of this report, the FBI indicated that the document shown in Exhibit 1 was only intended to be an "outline" for the gap analysis that was performed. However, recognizing that its gap analysis was not otherwise documented, the FBI informed us that it is preparing a "crosswalk" that will demonstrate how the vulnerabilities listed in the *Anatomy of a Case* were covered during the gap analysis and how they tie to the relevant action items in the mitigation plan. In instances where an identified vulnerability is not covered, the FBI

⁷ (U) Following its review of a draft of this report, the FBI informed us that it was seeking budget enhancements for UTS related risks.

⁸ (U) The full version of CD's *Anatomy of a Case* can be found in Appendix 6.

plans to document the acceptance of the associated risks posed by those vulnerabilities.

(U) Red Team Draft Mitigation Plan

(U//FOUO) Following its gap analysis, the Red Team process shifted to developing a plan to mitigate the risks created by the identified gaps in policy, [REDACTED], and training. According to OIC, participation by the divisions on the Red Team waned toward the end of the process and a smaller group of seven divisions focused on creating the mitigation plan. In addition to the regularly scheduled biweekly meetings of the entire Red Team, representatives from these seven divisions began meeting more frequently in order to make progress on the mitigation plan. As of the drafting of this report, the mitigation plan was not yet finalized. However, once completed, OIC plans to present the Red Team's report and draft mitigation plan to the Deputy Director's office for approval.

(S//NF) In September 2023, OIC provided us with a draft version of the mitigation plan which it said had already been reviewed by the Assistant Director of OIC and the Assistant Director of DI, but had not yet been approved by the Assistant Directors of the other participating divisions or their respective Executive Assistant Directors. The draft version of the mitigation plan that we reviewed consisted of [REDACTED] items organized into 6 categories, summarized in Table 1 below. Notably, more than 1 year later, in November 2024 (after the FBI's review of a draft version of this report), the FBI provided us with an updated version of the draft mitigation plan which included an [REDACTED] items for a total [REDACTED]. Due to the timing of this product, we did not analyze these additional action items prior to the finalization of this report.

(U) Table 1

(U) Summary of Red Team Draft Mitigation Plan as of September 2023

(U) Category	(U) Number of Action Items	(U) Example of an Action Item
(U) Policy	(S//NF) ■	(U) #1.4 - Update and finalize the Confidential Human Source Policy (CHSC) Guide.
(U) Procedures and Analysis	(S//NF) ■	(S//NF) ■
(U) Training	(S//NF) ■	(U) #3.17 - Provide UTS awareness training for all FBI employees, regardless of job series.
(S//NF) ■	(S//NF) ■	(S//NF) ■
(U) Monitoring	(S//NF) ■	(U) #5.1 - Establish a formalized UTS Executive committee to provide an ongoing review of the mitigation plan's implementation and evaluate ongoing changes in UTS.
(U) Auditing and Inspections	(S//NF) ■	(U) #6.1 - Assess completion rate of mandatory enterprise-wide, UTS-related training.

(U) Source: OIG Analysis of FBI data

(S//NF) In the full version of the draft mitigation plan we reviewed, each of the ■ items contained a short description of what needed to be accomplished, the entity responsible for completing the task, a target completion date, and the status of the progress made. Notably, while the draft mitigation plan included category headings for policy, training, and ■ that corresponded to the categories of the gap analysis outline, the plan did not explicitly link each action item in these categories to a vulnerability from the outline. As a result, it was not clear to us that the Red Team's gap analysis identified all potential vulnerabilities or that the draft mitigation plan's action items will address all vulnerabilities.

(S//NF) Based on our review of the draft mitigation plan, we also concluded that although some of the action items called for longer-term measures, overall, the plan did not adequately describe how the FBI would organize its UTS efforts after the steps detailed in the plan are completed and the Red Team and OIC are no longer involved. Rather, the draft plan consisted mostly of action items that would be completed in the short term. [REDACTED]

[REDACTED]. However, the draft mitigation plan contained no requirement that the [REDACTED] be conducted again in the future. We believe this is a significant shortcoming given the constantly evolving nature of the UTS threat, and a shortcoming that is present in many of the action items contained in the draft plan.

(S//NF) In response to our concerns about the lack of a longer-term structure for identifying and mitigating the UTS risk, OIC pointed to the "Monitoring" and "Auditing and Inspection" sections of the mitigation plan which listed action items focused on the future. For example, the "Monitoring" section included action items such as 5.1, which instructs DI to establish a formalized UTS Executive Committee to provide an ongoing review of the mitigation plan's implementation and evaluate ongoing changes in UTS, and the "Auditing and Inspections" section included action items such as incorporating UTS compliance factors into Field Office Inspections and requiring a review [REDACTED]. These may be future-focused, but we believe that without more specificity in the draft mitigation plan, these and similar action items may not be sufficient to establish clear, actionable strategies to address the UTS threat, or appropriate accountability for implementing those strategies.⁹

(U) Because of the discrepancy in the depth and breadth of vulnerabilities identified by the Red Team and those from *Anatomy of a Case*, we recommend that the FBI thoroughly document and incorporate all identified UTS vulnerabilities into its final UTS mitigation plan, including those identified in the *Anatomy of a Case*. This will help ensure that all UTS-related vulnerabilities identified by the OIC Red Team and other internal reviews are mitigated to the greatest extent possible.

(U) Development of the FBI's New UTS Strategic Plan

(S//NF) In November 2023, we met with the Executive Assistant Directors of each of the FBI's six branches to discuss the FBI's response to our December 2022 MAM and the preliminary findings of this audit, including our concerns about a lack of a strategic vision for addressing the evolving and ongoing threat posed by UTS. Shortly after our meetings with the Executive Assistant Directors, DI informed us that it was leading the development of an FBI-wide UTS Strategic Plan through a new UTS executive working group consisting of each of the seven FBI Divisions that participated in the development of the draft mitigation plan. [REDACTED]

[REDACTED]. Within each pillar was a description of the existing problems, why they are important, and the UTS goals within the pillar. According to DI, once finalized, the UTS Strategic Plan will be provided to the Deputy Director for approval and should complement the FBI's new 5-year national

⁹ (U) Due to the high-level nature of the Red Team's Gap Analysis and the other issues described in this report, we have thus far concluded that the Red Team's efforts were not sufficient to address the recommendation made in our 2022 MAM that the FBI complete an enterprise-wide threat assessment to identify all operational technology threats to the FBI's investigative and business practices. We will continue to work with the FBI to ensure the required steps are taken to close that recommendation.

intelligence program strategy and the FBI's overall Strategic Plan.

(U) Although we believe the new UTS Strategic Plan is an important step toward improving the FBI's UTS posture, we are concerned that the outline does not currently address how the disparate groups within the FBI that have developed expertise on UTS will be coordinated and effectively utilized. If this is not addressed, we believe there is a significant risk that these groups will duplicate each other's efforts and miss opportunities to collaborate, combine resources, and scale their efforts to the enterprise. Therefore, we recommend that, as the FBI finalizes its UTS Strategic Plan, it includes strategies for coordinating disparate UTS efforts found across the enterprise and leveraging existing resources that are already in place to address the evolving risks posed by UTS risks previously identified by the OIC Red Team and other internal reviews. In addition, the new Strategic Plan should ensure that FBI officials who have the authority to execute the strategy are identified and are empowered to ensure that the FBI has clear and unambiguous UTS-related policies throughout the enterprise.

(S//NF) Data Breach Exposes [REDACTED] Gaps in the FBI's Policies and Procedures for How to Respond to Such a Breach

(S//NF) [REDACTED] subsequent to our audit field work, we were made aware of a data breach [REDACTED]

(S//NF) FBI officials told us that when it was made aware of the breach, components throughout the FBI began assessing the risks to the enterprise that would likely result from the breach. [REDACTED]

(S//NF) [REDACTED]

(S//NF) [REDACTED]

¹⁰ (S//NF) [REDACTED]

[REDACTED]

(S//NF) The [REDACTED] officials with whom we spoke told us that, based on lessons learned during its response to this data breach, [REDACTED] is now developing a plan [REDACTED].

(S//NF) In our view, this incident illustrated many of the concerns identified in this report and, more generally, the high stakes of the UTS threat. According to the [REDACTED] officials' description of the incident and the FBI's response, it appears that due to practices the FBI previously identified as poor tradecraft and among the FBI's greatest vulnerabilities [REDACTED].

And notably, in our judgment neither the Red Team's Gap Analysis nor its draft mitigation plan provides guidance or action items that are specific enough to be likely to ensure that the FBI is significantly better positioned to respond should a similar breach occur in the future. Because of these issues, we recommend that the UTS Strategic Plan should also address the need for a clear line of authority for responding to UTS-related incidents.

(U) UTS-Related Training Efforts

(U) In response to the second recommendation in our December 2022 MAM, the FBI took steps to expand existing UTS training offerings and add additional UTS training for all of its personnel. Of particular note was the addition of a new, mandatory 45-minute UTS awareness training available to all FBI employees. According to the FBI, this UTS awareness training was to be completed by June 2024 and was offered both in-person and virtually through the FBI's Virtual Academy. Employees must take this training again every two years. The regularly provided 30-minute awareness briefing for all employees at *Onboarding New Employees* remained in place as well as a two-hour block of UTS training that is included in Basic Field Training Course at Quantico for new agent and intelligence analyst trainees.

(U) In addition to the basic UTS training offerings noted above, more advanced, optional training remains available to FBI agents through Human Intelligence Operations Training Unit on a limited basis. These include a consolidated, updated version of the UTS Training Course, HUMINT Intermediate Course, Advanced HUMINT Operations Course, and the Extraterritorial HUMINT Operations Course. These courses remain optional and DI told us that, due to limited resources, it can only offer those courses to a limited population of students. We believe ongoing training related to UTS is critically important, particularly for the FBI's agent ranks, and we are concerned about the low number of students served by the available advanced training courses. Therefore, we recommend that the FBI assess its ability to further expand the availability of its advanced UTS-related training modules and take any necessary additional steps to ensure all personnel are and remain adequately trained on both the basic and advanced skills they need to address the evolving UTS threat.

(U) Conclusion and Recommendations

(U) The FBI took an important step forward in addressing the threat posed by UTS in 2022 when former Director Wray established UTS as a "Tier 1 Enterprise Risk" and instructed the Office of Integrity and Compliance (OIC) to lead an enterprise-wide review of the risks posed by UTS. However, the resultant OIC-led Red Team and the gap analysis it performed appeared to identify only high-level gaps in the FBI's policy and training, potentially leaving unaddressed many UTS vulnerabilities to the FBI's personnel, investigations, and operations. Because the Red Team's subsequent draft mitigation plan was based on its gap analysis, we have corresponding concerns about that plan. We also have an independent concern about whether the draft mitigation plan will result in any mechanism at the FBI that will better position it to respond to the evolving UTS threat in the future, after the actions identified in the mitigation plan are complete and OIC is no longer directly involved in addressing the UTS threat.

(U) The FBI's current efforts to develop a UTS Strategic Plan that will complement its National Intelligence Plan and overall Strategic Plan represent another positive step, but an early outline of the strategy does not appear to identify officials who will have the authority to execute the strategy and ensure that the FBI has clear and unambiguous UTS-related policies throughout the enterprise. We are also concerned that the forthcoming strategy will not adequately create clear lines of authority when the FBI must respond to UTS-related security incidents. Finally, the FBI needs to make additional improvements to its training, as its more advanced UTS training modules are unable to serve many students who would benefit from them, suggesting this important training is still not reaching the personnel who need it most.

(U) We recommend that the FBI:

1. (U) Thoroughly document and incorporate all identified UTS vulnerabilities into its final UTS mitigation plan, including those identified in the *Anatomy of a Case*.
2. (U) Finalize its UTS Strategic Plan to include strategies for coordinating disparate UTS efforts found across the enterprise and leveraging existing resources that are already in place to address the evolving risks posed by UTS. In addition, the new Strategic Plan should ensure that FBI officials who have the authority to execute the strategy are identified and are empowered to ensure that the FBI has clear and unambiguous UTS-related policies throughout the enterprise.
3. (U) Establish a clear line of authority for responding to enterprise-wide, UTS-related incidents to ensure a coordinated response.
4. (U) Assess its ability to further expand the availability of its advanced UTS-related training modules and take any necessary additional steps to ensure all personnel are and remain adequately trained on both the basic and advanced skills they need to address the evolving UTS threat.

(U) APPENDIX 1: Objectives, Scope, and Methodology

(U) Objectives

(U) The objectives of our audit were to determine the sufficiency and effectiveness of: (1) the actions the FBI is taking to protect sensitive investigations and operations from technological compromise and whether those steps have been taken at the enterprise level, (2) training the FBI provides to its personnel to increase the work force's resiliency against technological compromise.

(U) Scope and Methodology

(U) Our audit generally covered, but was not limited to, the FBI's efforts to address risks and opportunities created by Ubiquitous Technical Surveillance between 2018 and January 2024. We reviewed the FBI's Confidential Human Source Policy Guide and the FBI's Domestic Investigations and Operations Guide. To accomplish our objectives, we interviewed 82 FBI officials including officials from the FBI's Counterintelligence Division, Counterterrorism Division, Criminal Investigative Division, Critical Incident Response Group, Cyber Division, Directorate of Intelligence, Facilities and Finance Division, Human Resources Division, International Operations Division, Laboratory Division, Office of General Counsel, Operational Technology Division, Security Division, Training Division, and the Weapons of Mass Destruction Directorate at FBI Headquarters.

(U) We conducted fieldwork at seven FBI field offices including Chicago, Columbia, Houston, New York, Philadelphia, Richmond, and Washington. We also met with officials at Redstone Arsenal in Huntsville, Alabama and the FBI Academy at Marine Corps Base Quantico. In addition, we met with officials at the Central Intelligence Agency and Defense Intelligence Agency to get a better understanding of tradecraft issues affecting other agencies in the Intelligence Community and how those agencies are addressing the issue.

(U) Statement on Compliance with Generally Accepted Government Auditing Standards

(U) We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) Internal Controls

(U) In this audit we performed testing, as appropriate, of internal controls significant within the context of our audit objectives. A deficiency in internal control design exists when a necessary control is missing or is not properly designed so that even if the control operates as designed, the control objective would not be met. A deficiency in implementation exists when a control is properly designed but not implemented correctly in the internal control system. A deficiency in operating effectiveness exists when a properly designed control does not operate as designed or the person performing the control does not have the necessary competence or authority to perform the control effectively.¹¹

¹¹ (U) Our evaluation of the FBI's internal controls was not made for the purpose of providing assurance on its internal control structure as a whole. FBI management is responsible for the establishment and maintenance of internal controls. Because we
Continued

(U) As noted in the Audit Results section of this report, we identified deficiencies in the FBI's internal controls that are significant within the context of the audit objectives and based upon the audit work performed that we believe may adversely affect the FBI's ability to protect its personnel, investigations and operations from risks posed by Ubiquitous Technical Surveillance. Specifically, we found no strategy to coordinate disparate efforts across the enterprise and that there was no clear line of authority to implement best practices related to the UTS threat.

(U) Compliance with Laws and Regulations

(U) In this audit we did not identify any laws or regulations governing the FBI's tradecraft or its response to Ubiquitous Technical Surveillance risks.

(U) Computer-Processed Data

(U) During our audit, we obtained information from Human Resources Division's HR Source system via the ThoughtSpot program. We used the data from this system to corroborate anecdotal information provided during interviews, however, we did not test the reliability of that system as a whole, therefore any findings identified involving information from that system was verified with documentation from other sources.

are not expressing an opinion on the FBI's internal control structure as a whole, this statement is intended solely for the information and use of the FBI. This restriction is not intended to limit the distribution of this report, which is a matter of public record. However, because this report contains sensitive information that must be appropriately controlled, a redacted copy of this report with sensitive information removed will be made available publicly.

(U) APPENDIX 2: Examples of the UTS Threat

(U) Examples of UTS Risks

(U) The FBI was aware of UTS risks being exploited by adversaries of the United States. The following real-world examples, provided to us by the FBI, illustrate consequences of poor tradecraft and the potential consequences of leaving the UTS threat unaddressed.

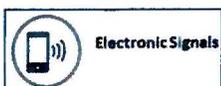
(U) Visual and Physical Imagery



(S//NF)

[REDACTED]

(U) Use of FBI Affiliated Electronic Communications



(S//NF)

[REDACTED]

(U) Financial Transactions

(U) Commercial entities regularly compile information from credit or debit card transactions to build profiles of consumers, and then sells this data to third parties who use it to build targeting advertising. Though this data is anonymized, in 2015, researchers from the Massachusetts Institute of Technology found that with the data from just four transactions, they could positively identify the cardholder 90% of the time.¹²

(S//OC/NF)



[REDACTED]

(U) Travel Data Correlation



(S//NF)

[REDACTED]

(S//NF)

[REDACTED]

¹² (U) MIT News, January 29, 2015, "Analysis: It's Surprisingly Easy to Identify Individuals from Credit-card Metadata," <https://news.mit.edu/2015/identify-from-credit-card-metadata-0129>.

[REDACTED]

(U) Online Presence and Electronic Communications



(U//FOUO) The leader of an organized crime family suspected an employee of being an FBI informant. To confirm this suspicion, the leader went through the call logs for the suspected employee's cell phone looking for phone numbers that may be connected to law enforcement. An online search of one of the phone numbers [REDACTED]

[REDACTED]

(U//FOUO) [REDACTED]



(S//NF)

[REDACTED]

(S//NF)

[REDACTED]

(U//FOUO) [REDACTED]



(S//OC/NF) Counterintelligence Division officials explained to us the importance of [REDACTED]

[REDACTED]

(U) Combination of Vulnerabilities



(U) In 2018, while the FBI was working on the "El Chapo" drug cartel case, an individual connected to the cartel contacted the FBI case agent. This individual said that the cartel had hired a "hacker" who offered a menu of services related to exploiting mobile phones and other electronic devices. In this particular case, the hacker observed people going in and out of the US Embassy in Mexico City and identified "people of interest" for the cartel, including the FBI Assistant Legal Attaché (ALAT).



Using the ALAT's mobile phone number the hacker was able to see calls made and received, as well as obtain the ALAT's geolocation data. According to the FBI, in addition to compromising the ALAT's phone, the hacker also accessed Mexico City's camera system,

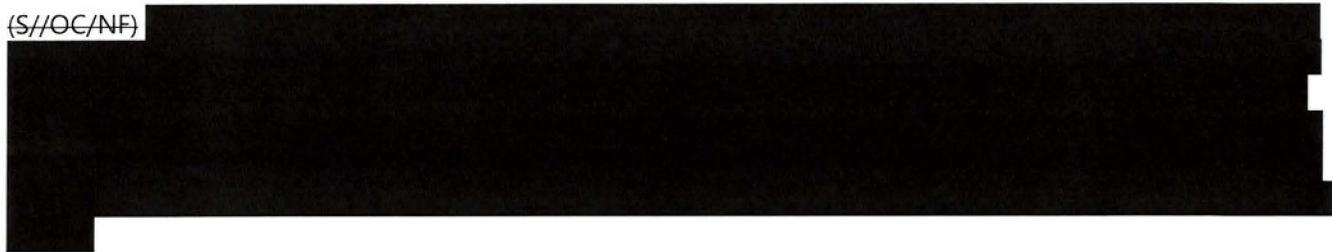
used the cameras to follow the ALAT through the city, and identified people the ALAT met with. According to the case agent, the cartel used that information to intimidate and/or kill potential sources or cooperating witnesses.

(U) APPENDIX 3: Lessons Learned by Other Government Agencies

(U) Risks resulting from UTS affect all government agencies, but they are especially acute in the agencies that comprise the US Intelligence Community.

(U) Central Intelligence Agency

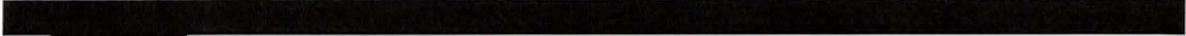
(S//OC/NF)



(S//OC/NF)

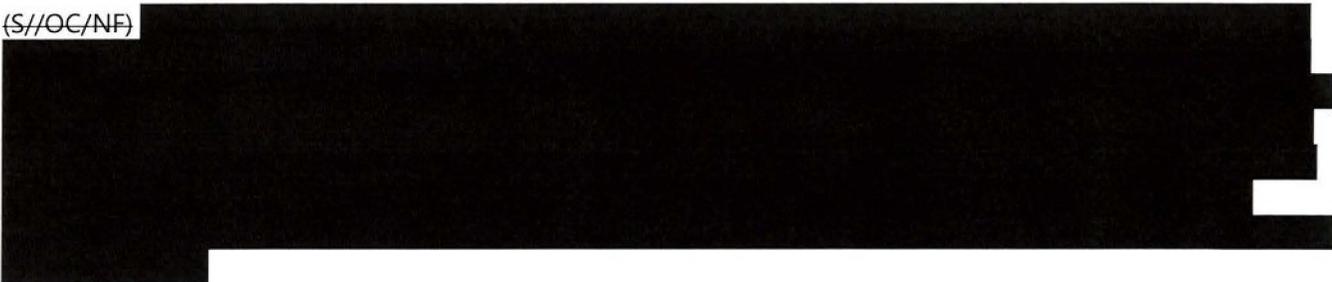









(S//OC/NF)



(U) Defense Intelligence Agency

(S//NF)



(S//NF)



(U) APPENDIX 4: FBI's Decentralized Attempts to Address UTS

(U) Counterterrorism Division's Advanced Projects Unit

(S//NF)

(U) International Operations Division's Strategic Intelligence Unit

(S//NF)

(U//FOUO)

(U//FOUO)

(U) New York Field Office

(S//NF)

(U) Washington Field Office

(S//NF)

(U) APPENDIX 5: Management Advisory Memorandum 23-013

~~SECRET//NOFORN~~



DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

(U) MANAGEMENT ADVISORY MEMORANDUM 23-013

(U) DECEMBER 2022

(U) Notification of Concerns Identified in the Federal
Bureau of Investigation's Response to Changing
Operational Technologies

~~Classified By: DOJIG567~~
~~Derived From: FBI NSICG~~
~~Declassify On: 20471231~~

AUDIT DIVISION

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~
MANAGEMENT ADVISORY MEMORANDUM

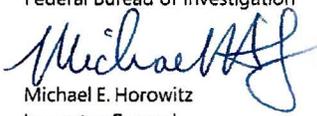


DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

December 19, 2022

Management Advisory Memorandum

To: Christopher A. Wray
Director
Federal Bureau of Investigation

From: 
Michael E. Horowitz
Inspector General

Subject: (U) Notification of Concerns Identified in the Federal Bureau of Investigation's
Response to Changing Operational Technologies

(U) The purpose of this memorandum is to advise you of certain deficiencies with the Federal Bureau of Investigation's (FBI) policies and procedures that the Office of the Inspector General (OIG) identified during an audit of the FBI's efforts to respond to changing operational technologies. Our preliminary objectives were to determine the sufficiency and effectiveness of: (1) the actions the FBI is taking to protect sensitive investigations and operations from technological compromise and whether those steps have been taken at the enterprise level, (2) training the FBI provides to its personnel to increase the work force's resiliency against technological compromise, and (3) counterintelligence policies and practices the FBI has developed to proactively use technological advancements to interrupt our adversaries' intelligence activities.

(U) We found that the FBI's response to the threats posed by changing operational technologies has been disjointed and inconsistent, and that the FBI needs an enterprise-wide approach to address this issue. In this memorandum, the OIG makes two recommendations to address the concerns we identified.

(U) The FBI's Response to Changing Operational Technologies Has Been Disjointed and Inconsistent

(U) Our preliminary audit work has included interviews with FBI personnel from the Office of General Counsel; the Operational Technology Division; the Directorate of Intelligence; the Counterterrorism Division; the Counterintelligence Division; and the New York, Philadelphia, and Washington Field Divisions.

(U//FOUO) Through these discussions we have learned that the threat posed by rapid changes in modern technology has made protecting sensitive operations, sources, and personnel very difficult. Advances in data mining and analysis, facial recognition, and computer network exploitation have made it easier than ever for nation state adversaries, terrorist organizations, and criminal networks to identify FBI personnel and operations.



MANAGEMENT ADVISORY MEMORANDUM

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~
MANAGEMENT ADVISORY MEMORANDUM

[REDACTED]

(S//NF) We determined that several entities within the FBI are addressing the issue of operational technology vulnerabilities. The Counterintelligence Division created a task force to address the issue and it has identified [REDACTED] vulnerability based on the FBI's current practices. The Operational Technology Division recognizes the significance of the risks posed by changing operational technologies and considers such risks when planning operations. The Directorate of Intelligence's Operational Security and Tradecraft Unit (OSTU) and Humint Operations Training Unit (HOTU) are also focused on addressing this urgent issue. However, these efforts appear to be [REDACTED]

[REDACTED] While HOTU offers training on proper technical tradecraft, that training is optional and only available for a limited number of FBI personnel due to budget and personnel constraints. There is no mandatory training FBI-wide other than [REDACTED]

(U//FOUO) Furthermore, based on our preliminary audit work, it appears that the [REDACTED]

Managers and field agents told us that there are [REDACTED]

(U) Enterprise-wide Efforts Need to Be Led from Outside of Operational Divisions

(U) Previous OIG audit work has shown that FBI efforts to address enterprise-wide issues from within a single division have been unsuccessful. The OIG's audit of the FBI's Insider Threat Program found that when the Insider Threat Center was a component of the Security Division it encountered significant challenges in getting support from the other divisions, thereby impeding the implementation of its mission. An enterprise-wide solution was not achieved until the Center was moved from the Security Division to the Associate Deputy Director's Office. Our Audit of the FBI's National Security Undercover Operations Program found similar issues with the National Covert Operations Section (NCOS) being located within the Criminal Division. The NCOS has had difficulty establishing itself as the enterprise-wide lead for covert operations support because the national security operational divisions view NCOS's expertise as being focused on criminal investigations. During our Audit of the FBI's National Security Undercover Operations Program, we also learned of efforts to create an Office of Tradecraft within the Directorate of Intelligence. This office was designed to address the issues raised in this memorandum, but this effort did not gain traction, in part, because the Office of Tradecraft would have been established in a single division.

(S//NF) In addition, during the current audit, we learned that, in recent years, at least one partner agency has [REDACTED]

[REDACTED] That agency stated that changing operational technologies are an existential risk and affect the entire intelligence community. Officials from this agency described its enterprise-wide coordination and the direction it received from its most senior executives as important factors in implementing its approach.

MANAGEMENT ADVISORY MEMORANDUM
~~SECRET//NOFORN~~

~~SECRET//NOFORN~~
MANAGEMENT ADVISORY MEMORANDUM

(U) Conclusion

(U//~~FOUO~~) We believe that the FBI needs an enterprise-wide, concerted effort to exploit the investigative and intelligence gathering opportunities created by technical tradecraft and to defend against the threat posed by changing operational technologies. As the FBI continues its efforts to address the threat posed to its personnel, investigations, and sources by operational technologies, we believe that the FBI can benefit from the lessons learned by other agencies and previous unsuccessful FBI efforts to address enterprise-wide issues from within one division. To communicate the gravity of this issue to everyone in the organization and emphasize an enterprise-wide approach, the FBI should conduct an enterprise-wide threat assessment to identify all operational technology threats to the FBI's investigative and business practices. The results of this threat assessment and options to mitigate the identified threats should be reported to the Deputy Director to assist the FBI in developing an enterprise-wide strategy for managing this risk. All FBI personnel should receive baseline training that informs them of the threats posed by changing operational technologies. [REDACTED]

(U) Recommendations

(U) We recommend that the FBI:

1. (U//~~FOUO~~) Perform a comprehensive, enterprise-wide assessment, with input from each division, to identify the operational technology threats to the FBI's investigative and business practices [REDACTED] develop options for an FBI-wide approach to mitigate each of the threats identified; identify [REDACTED] and report these options and the results of the assessment to the Deputy Director to use in developing and assigning responsibility for the FBI's enterprise-wide strategy for managing this risk.
2. (U//~~FOUO~~) Fully implement an enterprise-wide training plan for mitigating the threat posed to FBI investigations, personnel and sources by changing operational technologies. This training plan should include a baseline training for all employees, including non-agent personnel, [REDACTED]

(U) Please advise the OIG within 60 days of the date of this memorandum on what actions the FBI has taken or intends to take with regard to these issues. If you have any questions or would like to discuss the information in this memorandum, please contact me at (202) 514-3435 or Jason R. Malmstrom, Assistant Inspector General for Audit, at (202) 616-4651.

MANAGEMENT ADVISORY MEMORANDUM
~~SECRET//NOFORN~~

~~SECRET//NOFORN~~
MANAGEMENT ADVISORY MEMORANDUM

**(U) APPENDIX 1: The Federal Bureau of Investigation's
Response to the Draft Memorandum**

~~SECRET//NOFORN~~

November 10, 2022

To: Michael E. Horowitz
Inspector General

From: EAD Ryan Young *RY*
Intelligence Branch
Federal Bureau of Investigation

Subject: (U) Management Advisory Memorandum of October 11, 2022 Regarding
Concerns Identified in the Federal Bureau of Investigation's Response to
Changing Operational Technologies

Dear Inspector General Horowitz:

Thank you for the chance to respond to the Office of the Inspector General's (OIG) Management Advisory Memorandum, dated October 11, 2022 (the MAM), notifying the Federal Bureau of Investigation (FBI) of "Concerns Identified in the Federal Bureau of Investigation's Response to Changing Operational Technologies."

We agree that "the threat posed by rapid changes in modern technology has made protecting sensitive operations, sources, and personnel very difficult" and we recognize that the ongoing information revolution creates significant risks for the enterprise. [REDACTED]

[REDACTED] They originate moreover from individuals, criminal enterprises, terrorist organizations, and sophisticated nation-state actors, thus threatening both the FBI's law enforcement and national security missions.

As noted in the MAM, several divisions and other FBI entities are taking action responsive to this threat, including the Counterintelligence Division (CD), Operational Technology Division (OTD), and Directorate of Intelligence (DI). In addition to those expressly mentioned in the MAM, the Laboratory Division, and Cyber Division also play a critical role in exploiting and defending against these technologies. The FBI has, moreover, [REDACTED]

~~Classified By: G93K76B18~~
~~Derived From: FBI NSICG~~
~~Declassify On: 50Y1 RUM~~

~~SECRET//NOFORN~~

MANAGEMENT ADVISORY MEMORANDUM

~~SECRET//NOFORN~~

SECRET//NOFORN
MANAGEMENT ADVISORY MEMORANDUM

~~SECRET//NOFORN~~

The FBI's efforts have included:

- [REDACTED]

These and other efforts are detailed in an FBI document supplied to your office this past August, "FBI Efforts to Counter Ubiquitous Technical Surveillance."

[REDACTED]

[REDACTED]

FBI efforts have been multi-faceted and involved many components of the enterprise, working separately and in collaboration, including with other U.S. Government agencies facing similar threats. We nevertheless agree that to better understand the threat posed by changing operational technologies, an enterprise-wide assessment of threats posed by operational technology is warranted. This assessment should evaluate both investigative and business practices and should focus on threats to investigations, employees, operations, and Confidential Human Sources (CHSs). This assessment should seek to identify alternatives to mitigate these threats, including, where appropriate, solutions that might be applied enterprise-wide; and identify resource gaps that pose an obstacle to implementation.

[REDACTED]

~~SECRET//NOFORN~~

MANAGEMENT ADVISORY MEMORANDUM

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~
MANAGEMENT ADVISORY MEMORANDUM

~~SECRET//NOFORN~~

[REDACTED]

We also agree that all FBI personnel, both agents and non-agents, should be trained in the nature of these threats and in foundational techniques that may be used to reduce risk. The UTS awareness and OPSEC training currently provided to all new FBI employees is a start, but we recognize that this training must continually evolve as technologies change, adversaries adapt, and new mitigation tools and techniques become applicable to the entire workforce.

We further note that, while not all intelligence and law enforcement activity authorized for use by the FBI is significantly threatened by the changing technological landscape, certain threats must be met with tools and techniques that are matched to specific requirements. Advanced training should be supplied where such training is cost-effective and where advanced tools and techniques can effectively be put to use. [REDACTED]

[REDACTED] The enterprise-wide assessment should also assess resources needed to provide such matched trainings and to ensure the curriculum keeps pace with adversary tradecraft and evolving technology.

Again, we appreciate the opportunity to respond and will keep your office apprised as progress on these efforts proceeds.

~~SECRET//NOFORN~~

MANAGEMENT ADVISORY MEMORANDUM

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~
MANAGEMENT ADVISORY MEMORANDUM

**(U) APPENDIX 2: Office of the Inspector General Analysis
and Summary of Actions Necessary to
Close the Management Advisory Memorandum**

(U) The OIG provided a draft of this management advisory memorandum (MAM) to the Federal Bureau of Investigation (FBI). The FBI's response is incorporated in Appendix 1 of this final MAM. In response to our MAM, the FBI concurred with all of our recommendations. As a result, the status of the MAM is resolved. The following provides the OIG analysis of the response and summary of actions necessary to close the MAM.

(U) Recommendations for the Federal Bureau of Investigation:

1. **(U//FOUO) Perform a comprehensive, enterprise-wide assessment, with input from each division, to identify the operational technology threats to the FBI's investigative and business practices [REDACTED] develop options for an FBI-wide approach to mitigate each of the threats identified; [REDACTED] that pose an obstacle to full implementation; and report these options and the results of the assessment to the Deputy Director to use in developing and assigning responsibility for the FBI's enterprise-wide strategy for managing this risk.**

~~(S//NF)~~ Resolved. The FBI agreed with our recommendation. The FBI stated in its response that to better understand the threat posed by changing operational technologies, an enterprise-wide assessment of threats posed by operational technology is warranted and should: [REDACTED]

[REDACTED] The identified EAD will lead the enterprise with other EADs with approval by the Director.

(U//FOUO) The OIG will consider whether to close this recommendation when we receive evidence that the FBI has performed a comprehensive, enterprise-wide assessment, with input from each division, to identify the operational technology threats to the FBI's investigative and business practices [REDACTED] develop options for an FBI-wide approach to mitigate each of the threats identified; [REDACTED] that pose an obstacle to full implementation; and report these options and the results of the assessment to the Deputy Director to use in developing and assigning responsibility for the FBI's enterprise-wide strategy for managing this risk.

2. **(U//FOUO) Fully implement an enterprise-wide training plan for mitigating the threat posed to FBI investigations, personnel and sources by changing operational technologies. This training plan should include a baseline training for all employees, including non-agent personnel, [REDACTED] It should also include appropriate refresher training on a regular basis.**

(U//FOUO) Resolved. The FBI agreed with our recommendation. The FBI stated in its response that all FBI personnel, both agents and non-agents, should be trained in the nature of these threats and in

MANAGEMENT ADVISORY MEMORANDUM
~~SECRET//NOFORN~~

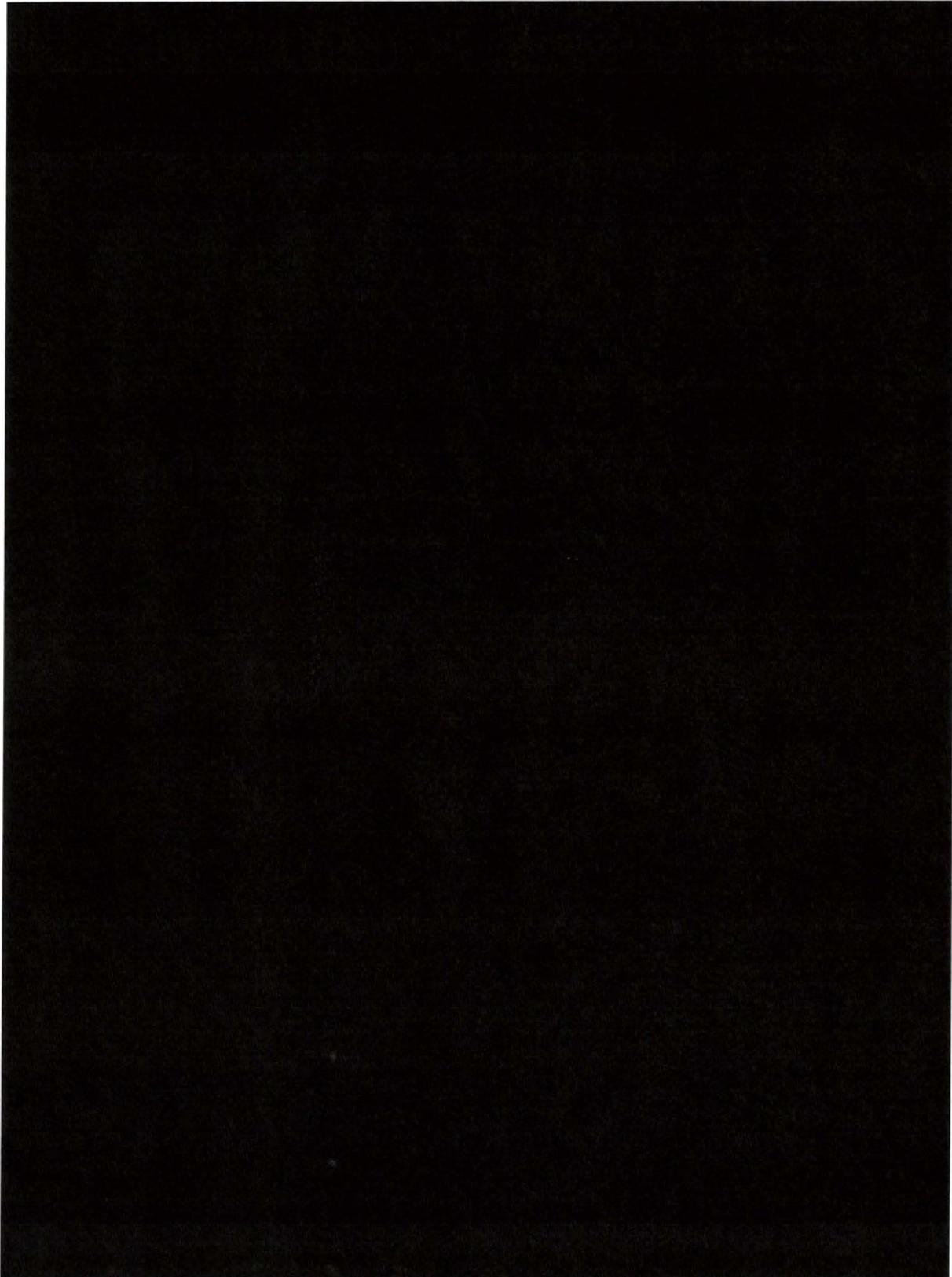
~~SECRET//NOFORN~~
MANAGEMENT ADVISORY MEMORANDUM

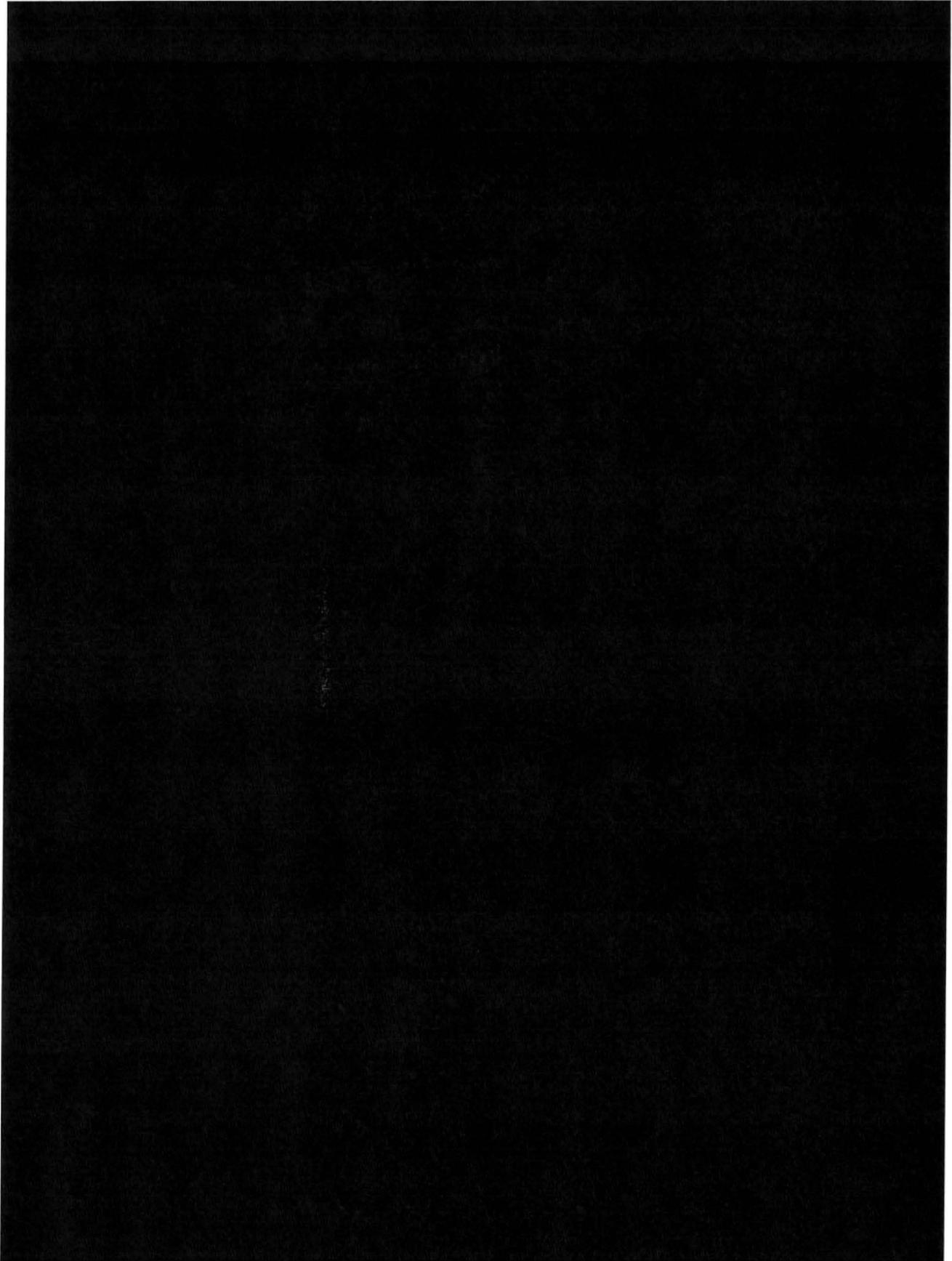
foundational techniques that may be used to reduce risk. [REDACTED]

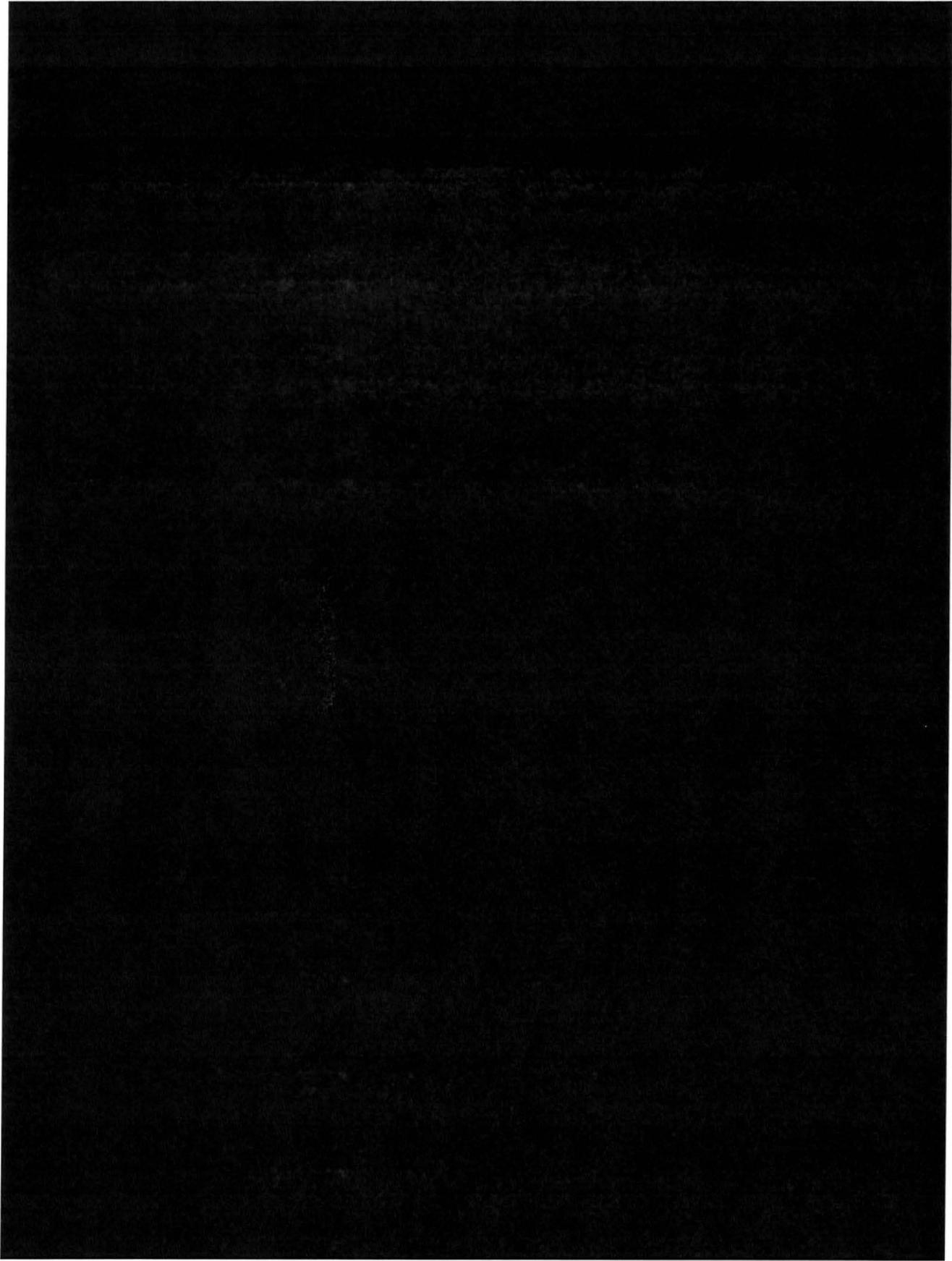
(U//~~FOUO~~) The OIG will consider whether to close this recommendation when we receive evidence that the FBI fully implemented an enterprise-wide training plan for mitigating the threat posed to FBI investigations, personnel and sources by changing operational technologies. This training plan should include a baseline training for all employees, including non-agent personnel, [REDACTED]. It should also include appropriate refresher training on a regular basis.

MANAGEMENT ADVISORY MEMORANDUM
~~SECRET//NOFORN~~

(U) APPENDIX 6: CD's Anatomy of a Case







(U) APPENDIX 7: Acronyms

(U) ALAT	(U) Assistant Legal Attaché
(U) CD	(U) Counterintelligence Division
(U) CHS	(U) Confidential Human Source
(U) CIA	(U) Central Intelligence Agency
(U) CMA	(U) Commercial Messaging Application
(U) DI	(U) Directorate of Intelligence
(U) DIA	(U) Defense Intelligence Agency
(U) FBI	(U) Federal Bureau of Investigation
(U) HUMINT	(U) Human Intelligence
(U) MAM	(U) Management Advisory Memorandum
(U) OIC	(U) Office of Integrity and Compliance
(U) OIG	(U) Office of the Inspector General
(U) OSTU	(U) Operational Security and Tradecraft Unit
(U) RTR	(U) Regional Tradecraft Review
(U//FOUO) [REDACTED]	(U//FOUO) [REDACTED]
(U) TTC	(U) The Tradecraft Center
(U) USG	(U) United States Government
(U) UTS	(U) Ubiquitous Technical Surveillance

(U) APPENDIX 8: The Federal Bureau of Investigation's Response to the Draft Audit Report



U.S. Department of Justice
Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 18, 2025

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, Audit of The Federal Bureau of Investigation's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance.

We look forward to working with the Office of the Inspector General to address the recommendations provided in the report. The FBI will take corrective actions to improve how it responds to the evolving UTS threat. We appreciate your feedback as we continue this effort.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Tonya Ugoretz".

Tonya Ugoretz
Assistant Director
Directorate of Intelligence

UNCLASSIFIED//~~FOUO~~

**The Federal Bureau of Investigation's Response to the
Office of the Inspector General's Audit of the Federal Bureau of Investigation's Efforts to
Mitigate the Effects of Ubiquitous Technical Surveillance**

Recommendation 1: Thoroughly document and incorporate all identified UTS vulnerabilities into its final UTS mitigation plan, including those identified in the *Anatomy of a Case*.

FBI Response to Recommendation 1: (U//~~FOUO~~) The FBI's UTS audit Red Team, led by the Office of Integrity and Compliance (OIC) and the Directorate of Intelligence (DI) identified all past and current ongoing efforts the FBI has in place to mitigate risk from UTS threats. Each division identified and provided their UTS policies and procedures currently in place. Once the Red Team received every division's input, which was included in the draft Mitigation Plan (Mit Plan), each division provided where they thought the FBI's gaps were for UTS mitigation. These discussions were ongoing for several months as the Red Team drafted the Mitigation Plan to ensure all identified UTS vulnerabilities were incorporated and documented. The FBI's UTS Mit Plan is not a short term solution. Action items marked as "completed", reflects that particular action item has been put into place and is ongoing. The Mit Plan identifies all the FBI's ongoing and future efforts to mitigate threats from UTS. This includes all UTS mitigation efforts previously provided in response to the MAM.

(U//~~FOUO~~) Every item on the CD "Anatomy of a Case" document is already incorporated into the FBI's UTS mitigation efforts. These vulnerabilities are covered by the action item categories in the Mit Plan. On 02/27/25, the DI's HUMINT Operations Section (HOS) and OIC demonstrated this to OIG in the form of a "crosswalk" excel spreadsheet. Each item from the CD "Anatomy of a Case" was cross-referenced to specific action items in the Mit Plan, addressing the UTS vulnerabilities concern.

(U//~~FOUO~~) There are items on the "Anatomy of a Case" where the risk is accepted. For example, [REDACTED]

[REDACTED] Any potential risk is mitigated through FBI employee general awareness of UTS, referenced in the training action items for the Mit Plan [REDACTED]

[REDACTED] In this circumstance potential risk is also mitigated through FBI employee general awareness of UTS, referenced in the training action items for the Mit Plan [REDACTED] Travel is one of the five UTS vectors, [REDACTED]

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Recommendation 2: Finalize its UTS Strategic Plan to include strategies for coordinating disparate UTS efforts found across the enterprise and leveraging existing resources that are already in place to address the evolving risks posed by UTS. In addition, the new Strategic Plan should ensure that FBI officials who have the authority to execute the strategy are identified and are empowered to ensure that the FBI has clear and unambiguous UTS-related policies throughout the enterprise.

FBI Response to Recommendation 2: (U//~~FOUO~~) The UTS Strategic Plan is being coordinated with other stakeholder divisions, and the DI will solicit feedback on both the overall plan and their respective division's anticipated role. The last phase of strategy development will integrate the feedback gathered from stakeholder divisions to create a finalized document that

[REDACTED]

(U//~~FOUO~~) FBIHQ divisions each own their respective mission and responsibilities for UTS mitigation. The Mitigation Plan identifies the division's respective action items, and where they should collaborate with different division partners. The FBI understands that, to some extent, efforts may appear duplicative, due to each division having its respective part to effect in UTS risk mitigation, therefore multiple divisions may be required to take the same action.

[REDACTED]

[REDACTED]

Deconfliction and coordination with regard to UTS efforts happens on a continuing basis through the UTS Executive Working Group, cross-divisional training opportunities, and in response to significant events [REDACTED]

Recommendation 3: Establish a clear line of authority for responding to enterprise-wide, UTS-related incidents to ensure a coordinated response.

FBI Response to Recommendation 3: (U//~~FOUO~~) The Deputy Director has the authority to execute the strategy, and the responsibilities fall under each Assistant Director's division, depending on their mission set. The clear lines of authority are established through the Branches' divisions' responsibilities and equities. Given the broad nature of this risk, the FBI has not assigned one individual executive to handle responding to enterprise-wide UTS incidents. In such cases, the Deputy Director will need the benefit of input from all branches of the FBI to ensure the Deputy Director had the information he needs to direct the enterprise-wide response.

Recommendation 4: Assess its ability to further expand the availability of its advanced UTS-related training modules and take any necessary additional steps to ensure all personnel are and remain adequately trained on both the basic and advanced skills they need to address the evolving UTS threat.

FBI Response to Recommendation 4: (U//~~FOUO~~) The FBI assessed the additional funding and resources required to provide advanced UTS training to all levels of personnel. [REDACTED]

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

All Employee UTS Training (AEUT)

The DI provided the AEUT via in-person sessions, live Skype conference calls, and a recorded version was released on Virtual Academy.

(U//~~FOUO~~) Also in FY24, the DI developed and implemented two new UTS trainings; the Operational Preparedness Course (OPC) and the Intermediate UTS Course (IUC).

(U//~~FOUO~~) The DI incorporated UTS mitigation into all the HUMINT training provided by the HUMINT Operations Training Unit (HOTU).

HUMINT Intermediate Course (HIC)

This course is targeted for Special Agents from all career paths and select FBI TFOs.

(U//~~FOUO~~) The DI also provides the Advanced HUMINT Operations Course (AHOC).

(U//~~FOUO~~) For additional advanced UTS training, the DI offers the Extraterritorial HUMINT Operations Course (EHOC).

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

[REDACTED]

(U//~~FOUO~~)

[REDACTED]

In the DI's FY25 and FY26 funding enhancement requests to the Department of Justice, the division requested additional funding and personnel to expand the number of courses offered each fiscal year. Both enhancement requests were denied. The DI will continue to request additional resources to further expand the availability of its advanced UTS-related training modules, and take any necessary additional steps to ensure all personnel are and remain adequately trained on both the basic and advanced skills they need to address the evolving UTS threat.

UNCLASSIFIED//~~FOUO~~

(U) APPENDIX 9: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Audit Report

(U) The OIG provided a draft of this audit report to the Federal Bureau of Investigation (FBI). The FBI response is incorporated in Appendix 8 of this final report. In response to our audit report, although the FBI did not agree or disagree with our recommendations, it stated that it looked forward to addressing the recommendations and that it will take corrective action to improve how it responds to the evolving UTS threat. As a result, the status of the audit report is resolved. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

(U) Recommendations for the Federal Bureau of Investigation:

1. (U) Thoroughly document and incorporate all identified UTS vulnerabilities into its final UTS mitigation plan, including those identified in the Anatomy of a Case.

(U) Resolved. The FBI neither concurred nor disagreed with the recommendation. The FBI stated that it looks forward to addressing the recommendations and that it will take corrective action to improve how it responds to the evolving UTS threat. Subsequent to the issuance of the draft report, the FBI provided us with a completed "crosswalk" to demonstrate that all vulnerabilities in the *Anatomy of a Case* were either addressed in the mitigation plan or deemed acceptable risks.

(U) The creation of the crosswalk demonstrating that all identified vulnerabilities were either addressed in the mitigation plan or deemed acceptable risks satisfies the intent of our recommendation, however the mitigation plan is still in draft form. Once we receive evidence that the mitigation plan has been approved and finalized with all identified vulnerabilities accounted for, the recommendation can be closed.

2. (U) Finalize its UTS Strategic Plan to include strategies for coordinating disparate UTS efforts found across the enterprise and leveraging existing resources that are already in place to address the evolving risks posed by UTS. In addition, the new Strategic Plan should ensure that FBI officials who have the authority to execute the strategy are identified and are empowered to ensure that the FBI has clear and unambiguous UTS-related policies throughout the enterprise.

(U) Resolved. The FBI neither concurred nor disagreed with the recommendation. The FBI stated that it is coordinating with the divisions to finalize the UTS strategic plan. As a result, this recommendation is resolved.

(U) This recommendation can be closed when we receive evidence that the FBI has finalized its UTS strategic plan, and appropriate FBI officials are given the authority to execute the strategy and ensure that clear and unambiguous UTS-related policies are in place throughout the enterprise.

3. (U) Establish a clear line of authority for responding to enterprise-wide, UTS-related incidents to ensure a coordinated response.

(U) Resolved. The FBI neither concurred nor disagreed with the recommendation. The FBI stated that the Deputy Director has the authority to execute the UTS strategy and ultimately has responsibility for responding to UTS incidents. As a result, this recommendation is resolved.

(U) This recommendation can be closed when we receive evidence of a policy or strategic document that establishes the Deputy Director as having the responsibility for responding to enterprise-wide UTS-related incidents to ensure a coordinated response.

4. (U) Assess its ability to further expand the availability of its advanced UTS-related training modules and take any necessary additional steps to ensure all personnel are and remain adequately trained on both the basic and advanced skills they need to address the evolving UTS threat.

(U) Resolved. The FBI neither concurred nor disagreed with the recommendation. The FBI stated that it is taking actions to address this recommendation, including creating new UTS courses and incorporating UTS mitigation into existing, advanced HUMINT courses, but noted that budget constraints hinder its ability to provide these trainings to all personnel that need them. As a result, this recommendation is resolved.

(U) Given the significance of the UTS threat to FBI personnel, operations, and investigations, this recommendation can be closed when we receive evidence that the FBI has expanded the availability of its advanced UTS-related trainings, or provides us with a plan for how available resources and funds will be used strategically to ensure that adequate basic and advanced trainings are provided to the personnel that need them.