



Audit of the Department of Justice's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance



AUDIT DIVISION

26-097

SEPTEMBER 2026

REDACTED FOR PUBLIC RELEASE

The full version of this report contains information that the Justice Management Division considered to be law enforcement sensitive and therefore could not be publicly released. To create this public version of the report, the Office of the Inspector General redacted (blackened out) portions of the full report.



(U) Audit of the Department of Justice's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance

(U) Introduction

(U) Department of Justice (Department or DOJ) employees engaged in every aspect of the Department's mission depend on technology and the use of online services to accomplish their work. However, for both individuals and organizations, these activities can create digital trails and discoverable connections that can be traced to users and organizations.

(U) Ubiquitous Technical Surveillance (UTS) refers to the capturing and analysis of such data to connect individuals to things, events, or locations. Such surveillance can present serious risks, including to the safety and security of individuals, organizations, and operations.

(U) The Federal Bureau of Investigation (FBI) has categorized the UTS threat into the following five vectors.

(U) Table 1

(U) UTS Vectors and Descriptions

(U) Vectors	(U) Description
(U) Visual and Physical	(U) Identification of people or objects tied to an operation through cameras or physical surveillance.
(U) Electronic Signals	(U) Use of electronic devices such as mobile phones.
(U) Financial	(U) Transactional financial records with unique identifiers linked to a specific account holder.
(U) Travel	(U) Records that include unique identifiers for hotel stays, border crossings, plane reservations, etc.
(U) Online	(U) Advertising data from web browsing and social media use, etc.

(U) Source: FBI

(U) In June 2025, the DOJ Office of the Inspector General (OIG) released a report on the FBI's efforts to mitigate the effects of UTS on its operations.¹ In that audit, we noted efforts by the FBI to address UTS risks and identified potential improvements for identifying and mitigating UTS-based vulnerabilities, coordinating FBI-wide UTS efforts, and providing UTS training. We also determined that the UTS-related issues faced by the FBI—and the UTS threat itself—likely affect the rest of the Department as well; therefore, we initiated this audit.

(U) Audit Objective

(U) The objective of this audit was to assess the Department's actions to address threats posed by UTS to the Department's operations and personnel.

(U) Results in Brief

(U) Complex UTS threats continue to affect the Department, yet we found that DOJ had no common definition of UTS and was not otherwise well-coordinated on the issue, few of the Department's components had taken action to mitigate the UTS threat, and UTS-specific training was lacking. We therefore concluded that the Department needs to ensure that all parts of the agency are taking action to mitigate and manage the risks that UTS presents to the safety of Department employees, and the security of its investigations, operations, and litigating activities.

(U) Based on the results of this audit, we make three [recommendations](#) to the Department to develop a coordinated UTS strategy, identify UTS risks and develop a plan to mitigate them, and improve UTS training for staff.

¹ (U) U.S. Department of Justice (DOJ) Office of the Inspector General (OIG), [Audit of the Federal Bureau of Investigation's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance](#), Audit Report 25-065 (June 2025), oig.justice.gov/reports/audit-federal-bureau-investigations-efforts-mitigate-effects-ubiquitous-technical.

(U) Prior OIG Audit of FBI Efforts to Mitigate the Effects of UTS and Actions Taken in Response

(U) In our 2025 audit of the FBI, we learned of specific instances where UTS had impacted the FBI's work. For example, while working on a drug cartel case, the FBI learned that the cartel had hired a "hacker" to exploit mobile phones and other electronic devices for call data and geolocation data, using that information to intimidate and, in some instances, kill potential sources or cooperating witnesses. In another example, the leader of an organized crime family used call logs stored in the cell phone of one of its business's employees to identify calls with a known FBI-issued cell phone. The FBI lost the source in that investigation.

(U) Our 2025 audit found that the FBI had taken several steps towards improving the protection of its employees, investigations, and operations against UTS. We also found areas in which those efforts needed to be enhanced. We identified the need for improvement in the identification of UTS risks affecting the FBI, coordination of efforts to mitigate those risks, FBI-wide strategic planning for addressing the ongoing risk, and UTS training for the workforce.

(U) In response to our findings, the FBI has taken several productive actions, including making UTS a "Tier 1 Enterprise Risk," conducting an FBI-wide review to identify UTS risks, developing a plan to mitigate those risks, and developing a UTS training plan tailored to employees across the organization. The FBI continues to work on a UTS strategic plan to coordinate its efforts enterprise-wide.

(U) Audit Results

(U) In the current audit, we determined that, outside of the FBI, the Department has not taken sufficient steps to manage the UTS threat. The OIG is concerned that the deficiencies identified in this audit place the Department and its employees, investigations, operations, sources, and witnesses at increased risk to UTS threats, and we believe the Department must improve its coordination and training on UTS to begin addressing the serious risks posed Department-wide.

(U) DOJ Needs a Coordinated Approach to Addressing the UTS Threat

(U) As in our 2025 audit of the FBI, during this audit we learned of recent instances where UTS had impacted the Department's work. Specifically, the Department told us of incidents in the past year involving the doxing of judges overseeing immigration cases managed by the DOJ Executive Office for Immigration Review (EOIR).² In these incidents, individuals gathered publicly available but sensitive information about the immigration judges from disparate sources and published that information in a manner that could be used for intimidation or other purposes. EOIR told us that such incidents require a coordinated response from the Department, including a security briefing for the affected judges from Department security personnel, the United States Marshals Service (USMS), and sometimes the FBI, at which these officials explain to the judges what risks they face. EOIR also uses a privacy and data removal service to try to remove as much of the judges' personal information as possible from the Internet.

(U) Despite such risks, which are not limited to immigration judges, based on our interviews with Department personnel from 12 non-law enforcement components and subcomponents, as well as 4 law enforcement components (including 32 subcomponents), we found a general lack of awareness and understanding of the UTS threat across the Department.³ We also found that, overall, the law enforcement components we audited were more aware of UTS threats than the non-law enforcement components.

(U//LES) [REDACTED]

[REDACTED]

² (U) "Doxing" has been defined by DOJ as, "the act of gathering, by licit and illicit means, and posting on the Internet personal identifying information ("PII") and other sensitive information about an individual, including, for example, addresses, dates of birth, social security numbers, telephone numbers, e-mail addresses, credit information, employers, and details regarding the individual's children and other family members."

³ (U) For the purposes of this audit, we considered the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Federal Bureau of Prisons (BOP); Drug Enforcement Administration (DEA); and U.S. Marshals Service (USMS) "law enforcement" components and all other components as "non-law enforcement" components. We did not include the FBI in this audit in light of our 2025 audit that focused on its efforts to mitigate the UTS threat.

(U) Table 2

(U//LES) [REDACTED]

(U//LES) [REDACTED]	(U//LES) [REDACTED]
(U//LES) [REDACTED] [REDACTED]	(U//LES) [REDACTED] [REDACTED] (U//LES) [REDACTED] (U//LES) [REDACTED] [REDACTED] (U//LES) [REDACTED] [REDACTED]
(U//LES) [REDACTED] [REDACTED]	(U//LES) [REDACTED]
(U//LES) [REDACTED] [REDACTED]	(U//LES) [REDACTED] (U//LES) [REDACTED] [REDACTED]
(U//LES) [REDACTED]	(U//LES) [REDACTED] [REDACTED] (U//LES) [REDACTED] [REDACTED]

(U//LES) [REDACTED]

(U//LES) Source: [REDACTED]

(U) We also found that DOJ has not taken any direct action at the enterprise-level to coordinate its components or to actively manage enterprise-level vulnerabilities. In addition, we found neither any individual nor office with explicit responsibility for coordinating the Department in addressing the UTS threat, nor any policy or other guidance explicitly addressing how the Department should coordinate on the issue. We therefore concluded that no single vehicle currently exists to ensure effective information sharing about known and emerging UTS threats and best practices to address the risks.⁴

(U) To begin addressing the UTS threat, we believe the Department would benefit from the development of a coordinated UTS strategy that defines UTS and establishes guidance on UTS threat identification and management.

(U) Specifically, we believe a common definition of UTS would aid the Department in increasing UTS awareness and helping facilitate the Department's ability to identify and manage its UTS-related vulnerabilities. In our previous audit of the FBI, we found that the FBI developed a definition of UTS that it used in informational briefings and trainings.⁵ This common definition created a shared understanding of the topic among different groups across the FBI's enterprise that we believe was critical to the FBI's ability to take coordinated action to combat the UTS threat. In comparison, of the 16 DOJ components and Department units we interviewed outside of the FBI, only the Drug Enforcement Administration's (DEA) Defensive Counterintelligence Unit had developed a

⁴ (U) We note that in response to our 2025 audit of the FBI's UTS efforts, the FBI created a "Red Team" consisting of representatives from each of its divisions to help address similar issues.

⁵ (U) DOJ OIG, *FBI's Efforts to Mitigate the Effects of UTS*, 1.

definition of UTS.⁶ A common definition of UTS will also enable the Department to take other crucial steps to mitigate the overall UTS risk, such as creating an inventory of specific UTS risks and developing a coordinated approach to track, prioritize, and mitigate each one.

(U) Defining the UTS threat, identifying vulnerabilities, and establishing a coordinated approach to mitigating the risks are critical steps in addressing this pressing issue, as they will allow the Department to align the expertise, funding, and priorities required to protect its employees, investigations, and operations from UTS risks.

(U) DOJ Needs to Improve Training for its Employees on the UTS Threat

(U) In response to our request, the Department identified 46 training courses offered to Department personnel during fiscal years 2024 and 2025 that it believed, based on keyword searches, were related to UTS.⁷ We determined that none of these trainings was UTS-specific, and while some of these trainings may have touched on topics relating to UTS, none described the threat posed by UTS, how to exploit UTS to the Department's benefit, or how to protect the Department from UTS risks.⁸ Additionally, only 7 of the 46 courses were mandatory, and the remaining voluntary courses were completed by less than 1 percent of non-FBI Department personnel.⁹ We therefore found that the Department did not provide baseline UTS awareness training to its employees or offer UTS-specific training, including advanced training for

employees in certain job functions such as surveillance, source handling, or counterintelligence.

(U) Given that the Department has no UTS-specific training and very low participation in the voluntary training courses that cover some aspects of UTS, we believe the Department's effort to ensure staff understand the UTS threat requires additional attention.

(U) Recommendations

(U) The threat posed by UTS puts the safety of Department employees, operational security of investigations and operations, and integrity of prosecutions at risk. Therefore, we recommend that the Justice Management Division:¹⁰

1. (U) Establish a coordinated UTS strategy that promulgates a common definition of UTS and assigns responsibility for managing the Department's UTS risk portfolio.
2. (U) To effectively manage the UTS risk portfolio, identify risks and develop a risk mitigation plan that, for each risk, assigns responsibility for determining and executing the Department's risk response.
3. (U) Create and implement a UTS training program that includes mandatory, basic UTS awareness training for all Department personnel, and advanced training for employees in specific job categories that are at higher risk of UTS-related threats.

⁶ (U) Based on experience and open-source reporting, the DEA Defensive Counterintelligence Unit defined UTS as, "the widespread and continuous collection of data through various technologies, often from everyday devices and activities, and to connect that data back to an individual."

⁷ (U) Subsequent to our testing, the Justice Management Division, Security and Emergency Planning Staff (SEPS) informed us of an additional course available to DOJ employees that it stated is applicable to the UTS threat, but we did not verify the content of the course prior to publishing this report.

⁸ (U) When the Department queried a list of training courses based on keyword searches relating to UTS, none of the courses directly mentioned or used the language "UTS" or "Ubiquitous Technical Surveillance."

⁹ (U) Mandatory Trainings included: DOJ – Information Technology Professional Training, Information Professional Training for Managers & Information Professional Training for Users; DEA – Foreign Travel Briefing; ATF – Counterintelligence Awareness and Security Training; USMS – Introduction to Operations Security & OPSEC Refresher Training.

¹⁰ (U) Since SEPS is responsible for enterprise-wide security, recommendations made in this report are addressed to JMD for implementation.

(U) APPENDIX 1: Audit Scope and Methodology

(U) Scope and Methodology

(U) To accomplish our objective, we sought DOJ policy and guidance related to UTS. We did not find any specific to UTS; however, we identified DOJ Order 1701, Security Programs and Responsibilities, as a policy that addresses the underlying issues related to UTS. In addition, we interviewed DOJ officials, including personnel from the Office of the Deputy Attorney General; Justice Management Division; National Security Division; Criminal Division; Executive Office for United States Attorneys; Organized Crime and Drug Enforcement Task Force; Civil Division; Executive Office for Immigration Review; Bureau of Alcohol, Tobacco, Firearms and Explosives; Federal Bureau of Prisons; Drug Enforcement Administration; and U.S. Marshals Service. We recently completed an audit of the Federal Bureau of Investigation's (FBI) efforts to mitigate the threat posed by UTS and therefore did not include the FBI in this audit.¹¹

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

(U) We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). 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 of internal controls significant within the context of our audit objectives. We did not evaluate the internal controls of the Department to provide assurance on its internal control structure as a whole. DOJ management is responsible for the establishment and maintenance of internal controls in accordance with OMB Circular A-123. Because we do not express an opinion on the Department's internal control structure as a whole, we offer this statement solely for the information and use of the Department.¹²

(U) As noted in the Audit Results section of this report, we identified deficiencies in the Department'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 Department's ability to protect its personnel, investigations, and operations from risks posed by UTS.

(U) The internal control deficiencies we found are discussed in the Audit Results section of this report. However, because our review was limited to those internal control components and underlying principles that we found significant to the objectives of this audit, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

(U) Compliance with Laws and Regulations

(U) In this audit we did not identify any laws or regulations governing the Department's response to UTS risks.

(U) Computer-Processed Data

(U) During our audit, we obtained information from various Department learning systems. These systems included the "LearnDOJ" system, BOP's "Bureau Learning University" system, USMS's "LearnUSMS" system, DEA's "DEA Learning System" and ATF's "Justice Talent Management" system. We did not test the reliability of those systems as a whole; therefore, any findings identified involving information from those systems were verified with documentation from other sources.

¹¹ (U) DOJ OIG, *FBI's Efforts to Mitigate the Effects of UTS*.

¹² (U) 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: The Department of Justice's Response to the Draft Report



U.S. Department of Justice

Justice Management Division

Security and Emergency Planning Staff

Washington, D.C. 20530

MEMORANDUM

TO: Thomas O. Puerzer
Regional Audit Manager
Philadelphia Regional Audit Office
Office of the Inspector General

FROM: James P. Baltimore
Director, Security and Emergency Planning Staff

JAMES

BALTIMORE

Digitally signed by
JAMES BALTIMORE
Date: 2026.09.14
12:59:38 -04'00'

SUBJECT: (U)Response to the Inspector General's Draft Audit Report, *The Department of Justice's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance*

- (U) The Security and Emergency Planning Staff (SEPS) appreciates the opportunity to review the Office of the Inspector General's (OIG) draft audit report titled, *The Department of Justice's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance* and provides the below response to the recommendations directed to SEPS.
- (U) **Recommendation No. 1: Establish a coordinated Ubiquitous Technical Surveillance (UTS) strategy that promulgates a common definition of UTS and assigns responsibility for managing the Department's UTS risk portfolio.**
- (U) *SEPS Response:* SEPS concurs with this recommendation and recognizes that UTS represents an evolving, enterprise-wide risk that crosses traditional security, counterintelligence, cybersecurity, information technology, operational security, privacy, and mission boundaries. Accordingly, the Department will develop and promulgate a coordinated UTS strategy and governance framework for managing UTS related risk.
- (U) The strategy will establish roles, responsibilities, authorities, and mechanisms for coordination among Department components with responsibilities or equities related to UTS. SEPS will provide enterprise-level coordination and oversight of the UTS risk portfolio while recognizing that responsibility for individual risks and implementation of specific risk responses may be based on components respective authorities, missions, and capabilities.
- (U) The strategy will also establish mechanisms for coordinating UTS activities across relevant disciplines, including physical and technical security, counterintelligence, cybersecurity, information security, operations security (OPSEC), privacy, acquisition and procurement,

MEMORANDUM FOR THOMAS O. PUERZER

(U) SUBJECT: Response to the Inspector General's Draft Audit Report, *The Department of Justice's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance* 2

information technology, and other affected mission areas. This governance model will provide centralized coordination and visibility of Department-wide UTS risk.

(U) **Recommendation No. 2: To effectively manage the UTS risk portfolio, identify risks and develop a risk mitigation plan that, for each risk, assigns responsibility for determining and executing the Department's risk response.**

(U) *SEPS Response:* SEPS concurs with this recommendation. As part of its enterprise UTS strategy, the Department will establish a structured process for identifying, assessing, prioritizing, mitigating, and monitoring UTS risks.

(U) The Department will develop and maintain a UTS risk portfolio that provides leadership with visibility into significant UTS threats, vulnerabilities, potential consequences, existing safeguards, and residual risks.

(U) For identified risks, the Department will develop a risk mitigation plan that:

- Identifies and describes the risk and affected Department missions, information, personnel, facilities, systems, or operations;
- Assesses the likelihood, potential impact, and relative priority of the risk;
- Identifies existing safeguards and risk-reduction measures;
- Identifies proposed mitigation measures and the Department's appropriate risk response;
- Assigns responsibility for implementing approved mitigation measures;
- Establishes milestones and measures for tracking implementation;
- Identifies residual risk following implementation of mitigation measures; and
- Establishes procedures for elevating significant risks requiring senior leadership decisions, additional resources, or formal risk acceptance.

(U) This approach will establish accountability while recognizing the multidisciplinary nature of UTS and preserving existing authorities and responsibilities.

(U) **Recommendation No. 3: Create and implement a UTS training program that includes mandatory, basic UTS awareness training for all Department personnel, and advanced training for employees in specific job categories that are at higher risk of UTS-related threats.**

(U) *SEPS Response:* SEPS concurs with this recommendation. The Department will develop and implement a tiered UTS training and awareness program designed to provide personnel with knowledge appropriate to their responsibilities and level of exposure to UTS related threats.

(U) The Department will establish baseline UTS awareness training for Department personnel. The training will provide a common understanding of UTS, examples of technologies and activities that may create UTS vulnerabilities, individual responsibilities for reducing exposure, appropriate protective practices, and procedures for reporting suspected UTS related incidents or concerns.

MEMORANDUM FOR THOMAS O. PUERZER

(U) SUBJECT: Response to the Inspector General's Draft Audit Report, *The Department of Justice's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance* 3

- (U) Enhanced training requirements will be established for personnel whose duties, access, travel, operational activities, or positions may place them at increased risk of UTS related targeting or exploitation. The Department will identify appropriate high-risk job categories through the UTS risk-assessment process rather than relying solely upon position title or component affiliation.
- (U) The Department will establish appropriate mechanisms for assigning, delivering, documenting, and periodically reviewing UTS training requirements to ensure training remains responsive to changes in technology, threat information, missions, and identified risks.
- (U) Collectively, these actions will establish an integrated Department-wide framework for managing UTS risk through governance, risk management, accountability, mitigation, training, and continuous assessment.

(U) APPENDIX 3: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Audit Report

(U) The Office of the Inspector General (OIG) provided a draft of this audit report to the Justice Management Division (JMD), Security and Emergency Planning Staff (SEPS). SEPS's response is incorporated in Appendix 2 of this final report. In response to our audit report, SEPS concurred with our recommendations and discussed the actions it will implement in response to our findings. 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 Justice Management Division (JMD):

1. **(U) Establish a coordinated Ubiquitous Technical Surveillance (UTS) strategy that promulgates a common definition of UTS and assigns responsibility for managing the Department of Justice's (DOJ or Department) UTS risk portfolio.**

(U) Resolved. SEPS concurred with our recommendation. SEPS stated that it will develop and promulgate a coordinated UTS strategy and governance framework for managing UTS-related risk. In addition, SEPS stated that the strategy will establish roles, responsibilities, authorities, and mechanisms for coordination among Department components with responsibilities or equities related to UTS. SEPS intends to provide enterprise-level coordination and oversight of the UTS risk portfolio.

SEPS also said that the UTS strategy will coordinate UTS activities across relevant disciplines, including physical and technical security, counterintelligence, cybersecurity, information security, operational security, procurement, and other affected mission areas.

(U) This recommendation can be closed when we receive evidence that SEPS has established a coordinated UTS strategy that promulgates a common definition of UTS and assigned responsibility for managing the Department's UTS risk portfolio.

2. **(U) To effectively manage the UTS risk portfolio, identify risks and develop a risk mitigation plan that, for each risk, assigns responsibility for determining and executing the Department's risk response.**

(U) Resolved. SEPS concurred with our recommendation. SEPS stated that as part of its enterprise UTS strategy, the Department will establish a structured process for identifying, assessing, prioritizing, mitigating, and monitoring UTS risks. The Department plans to develop and maintain a UTS risk portfolio that provides leadership with visibility into significant UTS threats, vulnerabilities, potential consequences, existing safeguards, and residual risks. The Department also plans to develop a risk mitigation plan that will identify and prioritize risks, propose mitigation measures, assign responsibility for implementation, identify gaps, and establish procedures for elevating significant risks to the attention of senior leadership.

(U) This recommendation can be closed when we receive evidence that SEPS has identified risks and developed a risk mitigation plan that, for each risk, assigns responsibility for determining and executing the Department's risk response.

3. (U) Create and implement a UTS training program that includes mandatory, basic UTS awareness training for all Department personnel, and advanced training for employees in specific job categories that are at higher risk of UTS-related threats.

(U) Resolved. SEPS concurred with our recommendation. SEPS stated that it plans to develop and implement a tiered UTS training and awareness program designed to provide personnel with knowledge appropriate to their responsibilities and exposure to UTS threats. In addition, the Department will establish baseline UTS awareness training for Department personnel and provide enhanced training requirements for personnel whose duties, access, travel, operational activities, or positions may place them at increased risk of UTS-related targeting or exploitation.

(U) This recommendation can be closed when we receive evidence that SEPS has created and implemented a UTS training program that includes mandatory, basic UTS awareness training for all Department personnel, and advanced training for employees in specific job categories that are at higher risk of UTS-related threats.