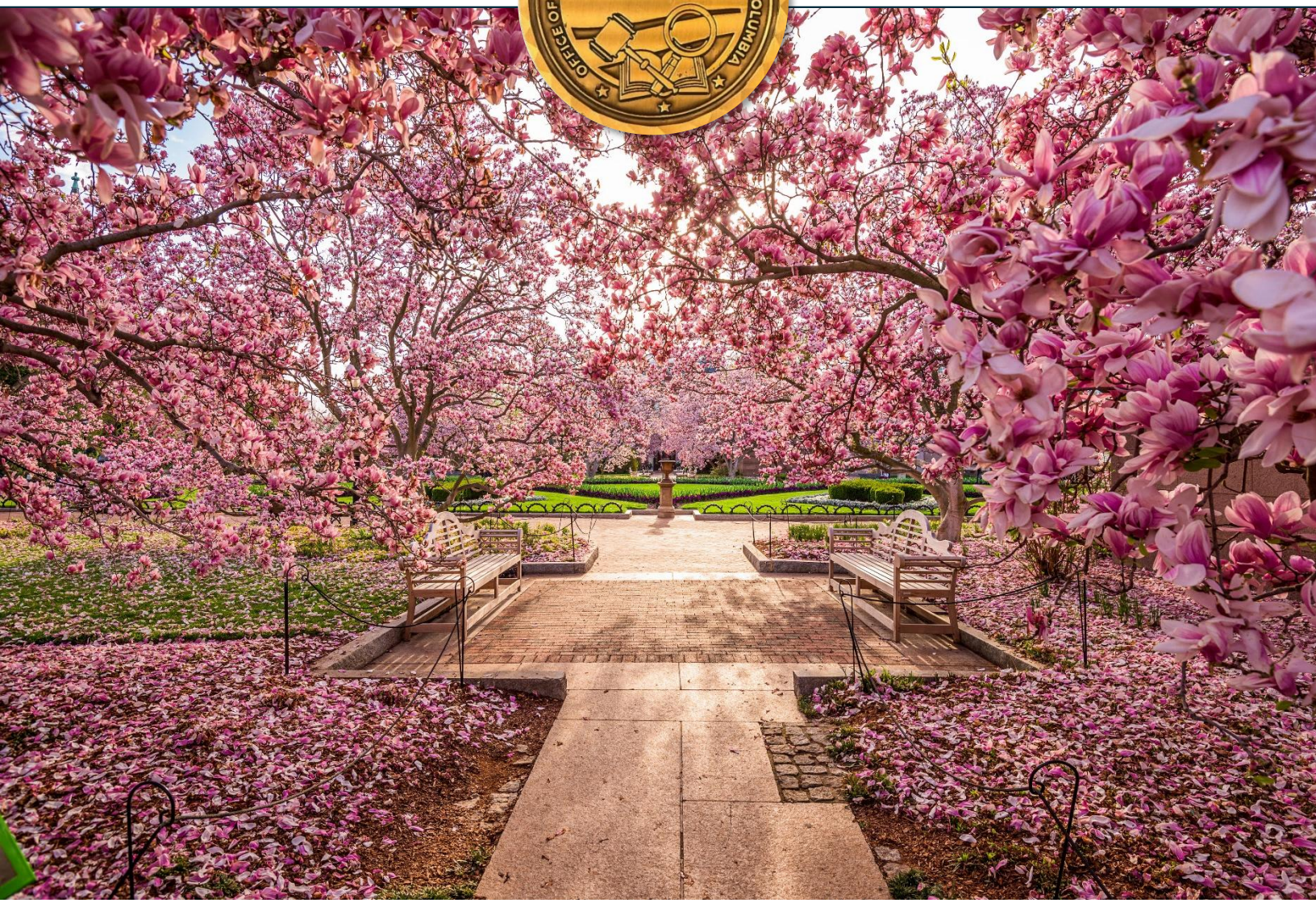
OFFICE OF THE
INSPECTOR GENERAL
DISTRICT OF COLUMBIA GOVERNMENT

INSPECTION REPORT

The Metropolitan Police Department's Crime Data Reporting Processes and Data Reliability Controls

OIG No. 26-E-03-FA0

July 28, 2026



MATTHEW WILCOXSON
INTERIM INSPECTOR MATTGENERAL

OUR MISSION

We independently audit, inspect, and investigate matters pertaining to the District of Columbia government in order to:

- prevent and detect corruption, mismanagement, waste, fraud, and abuse;
- promote economy, efficiency, effectiveness, and accountability;
- inform stakeholders about issues relating to District programs and operations; and
- recommend and track the implementation of corrective actions.

OUR VISION

We strive to be a world-class Office of the Inspector General that is customer focused and sets the standard for oversight excellence!

OUR VALUES

Accountability: We recognize that our duty extends beyond oversight; it encompasses responsibility. By holding ourselves accountable, we ensure that every action we take contributes to the greater good of the District.

Continuous Improvement: We view challenges not as obstacles, but as opportunities for growth. Our commitment to continuous improvement drives us to evolve, adapt, and enhance our practices.

Excellence: Mediocrity has no place in our lexicon. We strive for excellence in every facet of our work.

Integrity: Our integrity is non-negotiable. We act with honesty, transparency, and unwavering ethics. Upholding the public's trust demands nothing less.

Professionalism: As stewards of oversight, we maintain the utmost professionalism. Our interactions, decisions, and conduct exemplify the dignity of our role.

Transparency: Sunlight is our ally. Transparency illuminates our processes, decisions, and outcomes. By sharing information openly, we empower stakeholders, promote understanding, and reinforce our commitment to accountability.

MEMORANDUM

To: Jeffrey W. Carroll
Interim Chief of Police

From: Matthew Wilcoxson *Matthew Wilcoxson*
Interim Inspector General

Date: July 28, 2026

Subject: **The Metropolitan Police Department's Crime Data Reporting Processes and Data Reliability Controls**
OIG No. 26-E-03-FA0

This memorandum transmits our inspection report, *The Metropolitan Police Department's Crime Data Reporting Processes and Data Reliability Controls*. This inspection assessed the design, implementation, and operating effectiveness of MPD's internal controls over its crime classification and reporting processes, including its policies, procedures, supervisory oversight mechanisms, training practices, information systems, and organizational risk management. To accomplish this, we reviewed MPD crime data from calendar years 2015 through 2025.

We conducted this inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation*[1] and used *Standards for Internal Control in the Federal Government* (GAO Green Book) as our evaluative framework.[2] The OIG uses the standards in the GAO Green Book as criteria to assess the design, implementation, and operation of District internal control systems.

We made five recommendations to MPD aimed at improving its internal control framework for crime data collection, classification, and reporting. Implementing these recommendations fully—including adopting updated policies, information system controls, independent classification review, proactive risk assessments, and organizational culture

---

1 Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation*, (Washington, DC: CIGIE, 2020), https://www.ignet.gov/content/quality-standards-inspection-and-evaluation.

2 US Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-25-107721 (Washington DC: GAO, 2025), https://www.gao.gov/products/gao-25-107721, [GAO Green Book].

improvements—is essential to ensuring the reliability and integrity of MPD's crime data on an ongoing basis.

On July 23, 2026, MPD provided its response to our draft report. MPD agreed with all five recommendations and described actions taken and planned to implement them, including establishing an Office of Data Integrity and Analytics, auditing and restricting user access within Mark43, updating General Order 401.01, and incorporating crime reporting accuracy and policy currency into the Risk Management Division's audit cycle. MPD did not agree to include Office of Unified Communications calls for service data within the scope of its new review function; we address that in our note following Recommendation 1. We have included MPD's response in its entirety as Appendix 3.

We appreciate the cooperation and courtesy extended to our staff during this inspection. If you have any questions about this report, feel free to contact me.

The Metropolitan Police Department's Crime Data Reporting Processes and Data Reliability Controls

Summary

In December 2025, Mayor Bowser asked the DC Office of the Inspector General (OIG) to examine allegations that the Metropolitan Police Department (MPD) had been misclassifying and downgrading crimes. Rather than duplicate other ongoing investigations, the OIG focused on whether MPD had the systems, policies, and oversight in place to ensure its crime data is accurate. We reviewed MPD policies, interviewed officers and staff, rode along with patrol officers across all seven police districts, and analyzed crime data and incident reports from 2015 to 2025.

We found that MPD's crime reporting controls broke down significantly during the period we examined. An independent unit that reviewed crime reports for accuracy was shut down in 2013 and never replaced. The records system lacked basic controls over who could access and change data. Policies went years without updates. And the division responsible for identifying internal risks had never examined crime reporting accuracy.

Our inspection resulted in five recommendations focused on restoring independent oversight, strengthening system controls, modernizing outdated policies, and integrating crime data accuracy into MPD's risk-management and audit functions.

Objectives

Our goal was to assess whether MPD's policies, systems, training, and oversight mechanisms were designed and functioning to ensure that crime data is accurately classified and reliably reported to the public.

Recommendations

Our inspection produced three findings and one observation, from which we made five recommendations to the Chief of MPD. As detailed in this report, we recommend that the Chief:

- establish a permanent, independent crime report review function;
- implement a formal access control framework for the records management system;
- update policies governing crime classification, records management, and federal reporting;
- ensure crime reporting accuracy is assessed as part of the MPD's recurring audit cycle; and
- ensure policy currency is evaluated as part of the MPD's annual risk assessment.

Management Response

MPD agreed with all five recommendations. In its July 23, 2026, response, MPD described corrective actions already underway, including creating an Office of Data Integrity and Analytics with a dedicated Data Quality and Compliance Branch, auditing Mark43 user accounts and imposing interim permission restrictions while it works with the vendor on a permanent access control framework, consolidating crime reporting guidance into an updated General Order 401.01 *(Field Reporting System)*, and adding ongoing audits of crime reporting accuracy and data integrity daily by its Office of Data Integrity and Analytics. MPD did not agree to include analyzing the initial classification of calls for service data by the Office of Unified Communications within the scope of its new review function, and we ask MPD to reconsider that element. We consider MPD's planned actions otherwise responsive and will track implementation. MPD's response appears in its entirety in Appendix 3.

The Metropolitan Police Department's Crime Data Reporting Processes and Data Reliability Controls

Contents

BACKGROUND **1**

Historical Perspective on Crime Statistics 1

Importance of Crime Statistics 1

MPD's Role in Collecting and Reporting Crime Data 2

Reconciling District and Federal Crime Reporting 3

Noteworthy Actions 6

INSPECTION METHODOLOGY **7**

Why We Conducted This Inspection 7

Objective 7

Inspection Standards and Criteria 7

How We Conducted This Inspection 8

Scope and Limitations 9

KEY FINDINGS, RECOMMENDATIONS, AND OBSERVATIONS **10**

Finding 1: MPD Lacked a Cohesive Internal Control Framework for Crime Classification and Reporting 10

Finding 2: MPD Lacked Effective System Controls over its Records Management System (RMS) 15

Finding 3: Outdated Policies and the Lack of Proactive Risk Assessment Created Gaps in MPD's Crime Reporting Governance 19

Observation:MPD's Organizational Culture was Misaligned with its Published Values and Undermined its Crime Reporting Controls 22

CONCLUSION **24**

APPENDIX 1. FINDINGS **25**

APPENDIX 2. RECOMMENDATIONS **27**

APPENDIX 3. MANAGEMENT RESPONSE **30**

BACKGROUND

Historical Perspective on Crime Statistics

In 1930, Congress authorized the US Attorney General to gather crime information from various cities and state law enforcement agencies. In turn, the Attorney General designated the Federal Bureau of Investigation (FBI) as the central repository for reported crime information, using standardized offense classifications.[3]

In the early 1990s, law enforcement agencies began using crime statistics as a tool for proactive crime prevention. The New York City Police Department (NYPD) pioneered this approach with a data-driven performance system it called "Compstat," built around four core principles: collecting accurate and timely crime intelligence; deploying resources rapidly; implementing effective tactics; and conducting ongoing follow-up to hold commanders accountable.[4] The Metropolitan Police Department (MPD) adopted elements of the Compstat model beginning in 2002.[5]

Importance of Crime Statistics

Crime statistics play a central role in how the District understands and responds to public safety threats. They inform MPD's operational decision-making by separating actual crime trends from public perception, enabling the Department to identify emerging patterns, deploy patrol units strategically, evaluate crime reduction initiatives, and anticipate where additional resources may be needed. Accurate crime data also supports District leaders, community organizations, and other stakeholders who rely on MPD's publicly available data sets to evaluate programs, allocate funding, and provide services in the communities that need them most.

Crime statistics also serve a broader public purpose. Residents, stakeholders, researchers, federal partners, and the media use MPD's crime data to understand safety trends, evaluate government performance, and hold public agencies accountable. Publishing timely, reliable data helps ensure that discussions about crime are informed by accurate information rather than assumptions or anecdotes. Conversely, inaccurate or inconsistent crime data can erode public trust, distort both public understanding and policy discussions, and lead to inefficient deployment of resources.

---

3 Federal Bureau of Investigation, "About the Uniform Crime Reporting (UCR) Program," *Crime in the United States, 2010*, https://ucr.fbi.gov/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/aboutucrmain, accessed May 6, 2026.

4 Police Executive Research Forum, *Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies*, Bureau of Justice Assistance, U.S. Department of Justice, 2013, https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/PERF-Compstat.pdf.

5 Metropolitan Police Department, *Statistical Report 2001–2005: Using Data to Strategically Combat Crime*, 6, https://mpdc.dc.gov/sites/default/files/dc/sites/mpdc/publication/attachments/ar_2001_2005.pdf.

MPD's Role in Collecting and Reporting Crime Data

MPD is responsible for preventing crime, maintaining public order, enforcing District laws, and responding to calls for service across the city's seven police districts.[6] As part of these responsibilities, MPD collects, documents, classifies, and reports crime related information generated through officer interactions with the community.

Crime data collection begins with preliminary investigations and field reports, which officers complete when responding to or documenting an event. These reports capture the initial details known to MPD and form the basis for internal tracking, investigative follow-up, and offense classification.[7] After submission, incident reports undergo supervisory review (typically by sergeants and lieutenants) for completeness and proper crime classification, and certain offenses receive additional reviews from watch commanders or specialized investigative branches (e.g., homicides and sexual assaults).[8] MPD district commanders and data analysts may also conduct ad hoc reviews to ensure data accuracy and address emerging issues.[9] Once approved, data from incident reports populate MPD's public-facing "Crime Cards" system, the internal Daily Crime Reports, and the external Daily Crime Data at a Glance.[10] Throughout this report we will collectively refer to these as "MPD's crime data."

MPD and the Office of the Chief Technology Officer (OCTO) jointly maintain the data in the Crime Cards system. Crime Cards provides searchable, near real-time records of individual crime events dating back to 2009. MPD also publishes the same underlying incident data through the District's open data portal, making raw criminal incident records accessible for public analysis, academic research, media reporting, and civic technology applications. Both platforms are widely used for understanding neighborhood crime patterns and trends. Crime Cards organizes incidents by the date the offense is reported to MPD, which can influence how and when incidents appear in monthly or annual totals.

MPD produces crime data reports for both internal and external audiences. While both types of reports include the same underlying incident information, they differ in the level of detail provided. Internal crime data reports are distributed to district commanders and other MPD leadership and contain detailed, non-public information such as victim names, identifying information about persons of interest, and precise incident locations. These internal reports are generated separately for each police district and are used to guide daily operational decisions, resource allocation, and investigative follow-up. In contrast, the public-facing crime data reports

---

6 The seven police districts exclude federal properties and Metro stations, which fall under the primary jurisdiction of other law enforcement entities.

7 MPD General Order 401.01, *Field Reporting System,* 6-10, (GO-SPT-401.01, effective July 19, 2012), https://go.mpdconline.com/GO/GO_401_01.pdf.

8 For more information on MPD's ranks, see https://mpdc.dc.gov/sites/default/files/dc/sites/mpdc/publication/attachments/1.3%20Chain%20of%20Command.pdf.

9 MPD General Order 101.09, *Duties and Responsibilities of Sworn Officials* Part III.B.2(j) at 4 (GO-OMA-101.09, effective July 28, 2011), https://go.mpdconline.com/GO/GO_101_09.pdf.

10 *See* MPD, "DC Crime Cards," MPD, https://crimecards.dc.gov, (last visited June 1, 2026), and MPD, "District Crime Data at a Glance," MPD, https://mpdc.dc.gov/dailycrime, (last visited May 7, 2026).

published on MPD's website contains only aggregated, citywide counts of reported crime and excludes all sensitive information. This public version provides the community with a high-level snapshot of recent crime trends while safeguarding private information contained in the internal reports.

Reconciling District and Federal Crime Reporting

MPD also provides uniform crime reporting (UCR) data to the FBI's National Incident-Based Reporting System (NIBRS). Prior to 2021, MPD submitted monthly crime and arrest data to the FBI using criteria defined by UCR's Summary Reporting System (SRS). The eight UCR SRS Part 1 offense categories, with some important distinctions, generally align with the nine DC Code offense categories used in the Crime Cards system.

Figure 1. Comparison of DC Code and FBI UCR Part 1 Offense Definitions[11]

DC CODE INDEX OFFENSE DEFINITIONS	FBI UCR PART I CRIME DEFINITIONS
The MPD relies on the DC Code Index Offenses for daily operational and deployment decisions. Offenders who are arrested in the District of Columbia are prosecuted for the offenses represented in the DC Code.	The UCR provides a consistent measure of serious crime that can be compared across time periods or regions.
Homicide: Killing of another person purposely, in perpetrating or attempting to perpetrate an offense punishable by imprisonment, or otherwise with malice aforethought.	***Murder:*** The willful non-negligent killing of a person.
Sex Assault: One of many sexual acts against another person, either forcibly or without his/her permission, and/or against someone who is otherwise incapable of communicating unwillingness.	***Forcible Rape:*** Penetration, no matter how slight, of the vagina or anus with any body part or object, or oral penetration by a sex organ of another person, without the consent of the victim.
Robbery: The taking from another person, or immediate actual possession of another, anything of value, by force or violence, whether against resistance or by sudden or stealthy seizure or snatching, or by putting in fear. This category includes carjackings.	***Robbery:*** The taking or attempting to take anything of value from the care, custody, or control of a person or persons by force or threat of force or violence and/or by putting the victim in fear.
Assault with a Dangerous Weapon (ADW): Knowingly or purposely causing serious bodily injury to another person, or threatening to do so; or under circumstances manifesting extreme indifference to human life, knowingly engaging in conduct that creates a grave risk of serious bodily injury to another person, and thereby causes serious bodily injury. Weapons include, but are not limited to, firearms, knives and other objects.	***Aggravated Assault:*** An unlawful attack by one person upon another for the purpose of inflicting severe or aggravated bodily injury. This type of assault is usually accompanied by the use of a weapon or by means likely to produce death or great bodily harm.
Burglary: Breaking and entering, or entering without breaking, any dwelling, bank, store, warehouse, shop, stable, or other building or any apartment or room, whether at the time occupied or not, or any steamboat, canal boat, vessel, other watercraft, railroad car, or any yard where any lumber, coal, or other goods or chattels are deposited and kept for the purpose of trade, with intent to break and carry away any part thereof or any fixture or other thing attached to or connected with the same.	***Burglary:*** The unlawful entry of a structure to commit a felony or theft.
Theft/Other: This includes conduct previously known as larceny. The Theft/Other category excludes theft of items from a motor vehicle or the motor vehicle itself, which are captured under other categories, and excludes fraud.	***Larceny/Theft:*** The unlawful taking, carrying, leading or riding away of property from the possession or constructive possession of another.
Theft F/Auto: Theft of items from within a vehicle, excluding motor vehicle parts and accessories.	
Stolen Auto: Theft of a motor vehicle (any automobile, self-propelled mobile home, motorcycle, truck, truck tractor, truck tractor with semi trailer or trailer, or bus).	***Motor Vehicle Theft:*** The theft or attempted theft of a motor vehicle. "Motor vehicle" includes automobiles, trucks and buses, and other self-propelled vehicles that run on land surfaces and not rails.
Arson: The malicious burning or attempt to burn any dwelling, house, barn, or stable adjoining thereto, or any store, barn, or outhouse, or any shop, office, stable, store, warehouse, or any other building, or any steamboat, vessel, canal boat, or other watercraft, or any railroad car, the property, in whole or in part, of another person, or any church, meetinghouse, schoolhouse, or any of the public buildings in the District, belonging to the United States or to the District of Columbia.	***Arson:*** Any willful or malicious burning or attempt to burn, with or without intent to defraud, a dwelling house, public building, motor vehicle or aircraft, personal property of another, etc.

[11] MPD, *2019 Annual Report*, at 17, https://mpdc.dc.gov/sites/default/files/dc/sites/mpdc/publication/attachments/MPD%20Annual%20Report%202019__lowres.pdf. Note: Part I offenses are generally considered the most serious crimes.

In 2021, the FBI replaced the SRS with NIBRS, and MPD transitioned to NIBRS on August 1, 2021.[12] NIBRS captures all offenses within an incident, collects victim-level data, and applies the standardized UCR Part 1 offense definitions.

Structural differences mean that MPD's reported crime data and NIBRS use methodologies that make their data not directly comparable. For example, in 2025, MPD's Crime Cards reflected 126 homicides compared to NIBRS' 116.[13] Both counts are correct based upon their respective methodologies. Some important distinctions between MPD's crime data and NIBRS methodologies are below.

- **Offense Definitions:** MPD's crime data uses D.C. Code criminal offense definitions. NIBRS uses FBI offense definitions. While these definitions are mostly similar, there are meaningful differences in how crimes are defined between these two sources (e.g., when pepper spray is used in an assault, D.C. Code may consider this a "simple assault" whereas NIBRS would require it to be categorized as an "aggravated assault" due to the use of pepper spray).

- **Scopes of Reported Offenses:** MPD's crime data publicly reports nine offense categories. NIBRS captures dozens of additional offense types—such as animal cruelty, extortion, and identity theft—that never appear in MPD's public-facing crime data.[14]

- **Units of Measurement**: MPD's crime data counts criminal incidents—one count per reported event.[15] NIBRS counts victims, meaning that a single incident involving multiple victims generates multiple offense counts.[16]

---

12 Metropolitan Police Department, 2022 Annual Report, Appendix B, "FBI Uniform Crime Reporting Program: Migrating from SRS to NIBRS," 46, https://mpdc.dc.gov/sites/default/files/dc/sites/mpdc/publication/attachments/AR_2022_lowres.pdf (last visited May 7, 2026).

13 MPD, "Crime Cards," accessed May 15, 2026, https://crimecards.dc.gov/all:crimes/all:weapons/dated::01012025:12312025/citywide:heat; and FBI, "Crime Data Explorer," accessed May 15, 2026, https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/explorer/crime/crime-trend. All information in this section can be found at these locations, unless otherwise noted.

14 FBI, Uniform Crime Reporting Program: National Incident-Based Reporting System, "NIBRS Offense Codes," https://ucr.fbi.gov/nibrs/2011/resources/nibrs-offense-codes (last visited May 7, 2026). Note: "Group B" offenses included in these offense codes are only reported to NIBRS when they result in an arrest.

15 MPD General Order 401.01, Field Reporting System, Part IV.F at 5, (GO-SPT-401.01, effective July 19, 2012), https://go.mpdconline.com/GO/GO_401_01.pdf.

16 FBI, *NIBRS User Manual 2025.0, §* 2.2 "Classifying Offenses" at 19. https://le.fbi.gov/file-repository/nibrs-user-manual-2025-0-062625.pdf/view.

- **Hierarchy Rule:** MPD's crime data reports only the most serious offense in each incident, excluding all others.[17] NIBRS requires reporting on all offenses within a single incident, (up to ten).[18]

- **Inclusion of Other Agencies:** MPD is not the only agency that reports crime data to NIBRS for incidents occurring in the District. In NIBRS, each participating law-enforcement agency, such as the DC Fire and Emergency Medical Services or the Metro Transit Police, submits incidents that it responds to and records. As a result, the NIBRS data set reflects combined reporting from all participating agencies, not just MPD.[19] By contrast, MPD's crime data is drawn from MPD's own records management system and does not include incidents responded to and recorded by other agencies.[20]

- **Timing:** MPD's crime data is updated daily with real-time crime data and uses the report date, which reflects when the report was filed rather than when the crime occurred.[21] NIBRS data, by contrast, is submitted monthly to the FBI and uses the date of occurrence, offering a more complete and standardized accounting of when crimes took place, but without the immediacy of daily updates.[22] This makes MPD's crime data more responsive for near–real-time monitoring, though individual records may still be refined as investigations proceed.

Differences between MPD and NIBRS data do not, by themselves, indicate inaccuracies. They do, however, underscore the importance of strong internal controls to ensure that information entering each system is complete, accurate, and consistent with applicable classification standards.

Noteworthy Actions

Over the past several months, MPD took steps to address concerns in crime classification and reporting. For example, in February 2026, the Department developed and launched a mandatory training module focused on DC Code crime classification, specifically intended to better equip officers with the knowledge, skill, and ability to properly classify offenses. Also, while not yet operationalized, the Department is in the process of reestablishing its Staff Review Unit (SRU),

---

17 MPD General Order 401.01, Field Reporting System, Part IV.F at 5.

18 FBI, *NIBRS User Manual 2025.0, §* 2.2 "Classifying Offenses" at 19.

19 FBI, "Crime Data Explorer."

20 MPD, "District Crime Data at a Glance."

21 MPD, "Crime Cards: Frequently asked questions – What crimes are shown here?," accessed May 15, 2026, https://crimecards.dc.gov/all:crimes/all:weapons/dated::01012025:12312025/citywide:heat;

22 MPD, "Standard Operating Procedures: Investigative Case Tracking and UCR Classification," II.H at 17, (effective April 8, 2003), https://go.mpdconline.com/GO/SOP_investigative_case_tracking.pdf.

which had previously served to provide an independent, non-patrol set of examiners responsible for reviewing classification accuracy and report quality.[23]

INSPECTION METHODOLOGY

Why We Conducted This Inspection

On December 22, 2025, Mayor Bowser asked OIG to examine allegations of crime misclassification and downgrading at MPD. The request followed reports issued by both the House Committee on Oversight and Government Reform,[24] as well as a draft Memorandum of Investigation from the US Attorney's Office for the District of Columbia. To avoid duplicative efforts, we determined that the most productive path was to evaluate the integrity of MPD's policies and processes for crime reporting. Our inspection aimed to determine whether MPD's internal control system provides reasonable assurance that crime data is accurately classified and reliably reported, and to identify specific improvements needed to provide that assurance going forward.

Objective

The objective of this inspection was to assess the design, implementation, and operation of MPD's internal control system for collecting, classifying, and reporting crime data. Specifically, we examined whether MPD's policies, supervisory oversight, training, information systems, and monitoring mechanisms were designed and operating to ensure the reliability and integrity of MPD's crime reporting process.

Inspection Standards and Criteria

We conducted this inspection in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and used the *Standards for Internal Control in the Federal Government*—commonly known as the Green Book—as our evaluative framework. The Green Book defines what an effective internal control system looks like for government agencies, organizing requirements across five areas: the overall control environment, risk assessment, control activities, information and communication, and monitoring. These components and their supporting principles provided the criteria against which we assessed MPD's crime reporting controls. We also considered OMB Circular A-123,

---

[23] MPD General Order 401.01, Field Reporting System, Part VI.D.1-2 at 22, (GO-SPT-401.01, effective July 19, 2012), https://go.mpdconline.com/GO/GO_401_01.pdf

[24] US House Committee on Oversight and Government Reform, Leadership Breakdown: How D.C.'s Police Chief Undermined Crime Data Accuracy, interim staff report, Dec. 14, 2025, https://oversight.house.gov (press release and report summary available); US House Committee on Oversight and Government Reform, Democratic Staff, Exposing the False Claims Justifying the Trump Administration's Attacks on the Metropolitan Police Department: Evidence Demonstrates Significant Reduction in Crime in D.C. Since 2023, staff report, Dec. 19, 2025, https://oversightdemocrats.house.gov/.

Management's Responsibility for Internal Control, which requires agencies to conduct annual, risk-based assessments of internal controls and address any identified significant weaknesses.

Because MPD relies heavily on information systems to collect, classify, and report crime data, we also applied the *Federal Information System Controls Audit Manual* (FISCAM), a framework specifically designed to evaluate whether technology systems are properly secured, consistently configured, and accessible only to authorized users.[25] Applying FISCAM alongside the Green Book ensured that our assessment addressed both the human and technological dimensions of MPD's crime reporting controls.

How We Conducted This Inspection

Literature Review

Concerns about the accuracy and reliability of crime statistics are not unique to the MPD. Research has consistently found that when the same personnel responsible for crime reporting are also the ones whose performance is measured by that crime data, there is an inherent incentive to influence the numbers.

Our office reviewed research and reporting on NYPD's CompStat practices and allegations of crime statistics manipulation. Following whistleblower disclosures, NYPD commissioned an independent review of its crime reporting practices that produced recommendations to strengthen internal oversight.[26] Those findings informed our inspection approach.

Review of MPD Policies, Procedures, and Operational Records

We reviewed MPD's policies, procedures, and operational records governing crime classification and reporting, including general and special orders, standard operating procedures, training materials, organizational directives, supervisory-review requirements, crime data extracts, report samples, and classification guidance. This review formed the foundation for assessing whether MPD's policy framework accurately reflected its current organizational structure, systems, and operational expectations.

Interviews with MPD Sworn Officers and Professional Staff

We conducted thirty voluntary interviews across a range of ranks and operational and support units to understand how crime reporting procedures functioned in practice. Interviews provided direct insight into how offenses are classified; how reports are prepared, reviewed, and entered into MPD's records management system (RMS); how supervisory expectations are communicated;

---

[25] US Government Accountability Office, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, DC: GAO, 2009).

[26] David N. Kelley and Sharon L. McCarthy, *Report of the Crime Reporting Review Committee to Commissioner Raymond W. Kelly Concerning CompStat Auditing*, Apr. 8, 2013, https://home4.nyc.gov/assets/nypd/downloads/pdf/public_information/crime_reporting_review_committee_final_report_2013.pdf.

and how personnel experience challenges related to training, policy clarity, system limitations, and organizational culture. These perspectives helped identify gaps between written policy and operational practice and informed our assessment of control effectiveness.

Patrol Ride-Alongs

Members of the inspection team participated in the MPD Ride-Along Program, accompanying patrol members across several police districts during varying shifts. The ride-alongs provided direct insight into how crime reporting controls operated at the point of origin, including procedural variability across officers and districts, differences between written policy and field practice, and the real-world conditions under which officers classify and document offenses.

Incident Report Analysis

We reviewed and analyzed a structured sample of incident reports to assess whether officers and supervisors were following MPD's reporting standards, and data integrity requirements. We also examined report narratives and supervisory "rejection" comments to identify trends in report quality, completeness, and the corrective feedback provided to reporting officers. When we refer to rejection, we are referring to the feedback a supervisory officer gave to a subordinate to fix their report and resubmit it for review.

Scope and Limitations

Our inspection scope examined MPD's crime reporting policies, procedures, supervisory practices, information systems, and crime data governance structures. To understand long term trends and the operational context in which MPD's crime reporting process functions, we reviewed documentary and operational records covering calendar years 2015 through 2025. This scope allowed us to identify broad patterns relevant to internal control design and operation. It was not intended to determine the factual accuracy of specific incidents or assess the reliability of data previously reported by MPD.

KEY FINDINGS, RECOMMENDATIONS, AND OBSERVATIONS

Our overall assessment is that MPD experienced a prolonged, systemic breakdown of its internal control system for crime classification and reporting over our scope period (2015–2025). This report presents our findings and recommendations in three areas: the absence of an internal control framework, weaknesses in RMS system controls, and deficiencies in policy and risk governance. We also make one observation about misalignment between organizational values and goals.

Finding 1: MPD Lacked a Cohesive Internal Control Framework for Crime Classification and Reporting

An effective internal control framework for crime classification and reporting requires more than isolated policies or individual review mechanisms. It requires an integrated system in which leadership establishes clear authority and accountability; written policies accurately describe how the organization actually operates; personnel are trained to consistent standards; information systems enforce rather than permit compliance; and an independent oversight function monitors whether controls are present and functioning as designed. When any one element is absent or begins to deteriorate, the reliability of the system suffers.[27]

We found that MPD's internal control framework for crime classification and reporting had deteriorated over more than a decade.

- The Staff Review Unit, MPD's independent review function that served as the system's quality check, was disbanded and never replaced.
- The RMS transitioned without a documented process governing user permission.
- Policies went unrevised as the organizational structures and systems they described ceased to exist.
- The function charged with proactively identifying internal risks never assessed crime reporting accuracy.

No single failure caused the others, but together they reflect the absence of a functioning, cohesive internal control framework—one in which the parts were designed to work together and leadership had visibility into whether they did. The following subsections examine each area where the internal control framework did not function as intended.

---

[27] GAO Green Book, § OV2.04, which states, "[t]he five components of internal control must be effectively designed, implemented, and operating, and operating together in an integrated manner, for an internal control system to be effective."

The Former Staff Review Unit Provided a Centralized, Independent Quality Review Function

From 2013 through the time of this inspection, MPD did not maintain an independent, centralized review function to verify whether offense classifications matched the facts documented in report narratives. MPD previously relied on the Staff Review Unit (SRU) for this role, but the Department disbanded the unit around 2013 during its transition to a new RMS (Cobalt) and changes in reporting responsibilities. In the years that followed, limited review resources focused primarily on federal reporting compliance rather than classification accuracy, and key system controls in the RMS were absent. As a result, reports with classification errors or incomplete narratives could pass through the approval process uncorrected. MPD has begun evaluating options to reestablish an independent review capability.

The SRU operated as a centralized, non-patrol review function staffed by legal instrument examiners—civilian and limited-duty sworn personnel—whose primary role was to verify that offense classifications matched report narratives and that required data elements were complete. The unit had authority to reject reports and return them to the originating officer for correction.[28] Because the unit operated outside the patrol chain of command, its review was not subject to the same workload pressures, time constraints, and supervisory relationships that can affect the thoroughness of in-district review. Personnel familiar with the SRU described its function as a final consistency check before reports were finalized—one that helped minimize disparities in crime reporting and classification.

The SRU also served as the authoritative arbiter of classification disputes. The 2003 *Investigative Case Tracking and UCR Classification Standard Operating Procedure* (SOP) assigned the UCR Coordinator (a position within the SRU which required extensive knowledge of crime classification and District and federal laws) final decision-making authority over classification discrepancies between reporting officers, reporting sergeants, and the SRU itself. This made clear that the SRU was not simply a clerical check; it was the definitive voice on classification accuracy at the end of the approval process.

Without Independent Review, Classification Errors Could Go Undetected

In the absence of a centralized review unit, responsibility for identifying classification or narrative issues defaulted to district commanders and their supervisory teams, who already were subject to substantial operational demands and time pressures. As a result, there was no assurance that classifications were reviewed consistently or in a systematic manner. Several examples show how the detection of classification errors depended largely on individual initiative rather than structured oversight.

---

[28] MPD General Order 401.01, Field Reporting System, Part VI.D.1-2 at 22, (GO-SPT-401.01, effective July 19, 2012), https://go.mpdconline.com/GO/GO_401_01.pdf.

Without an independent review function, the Department lacked the mechanisms needed to ensure classification accuracy beyond initial supervisory checks. MPD did not systematically track rejection rates, classification corrections, or recurring error types across districts. No consolidated list of disputed reports existed, leaving the Department without a way to identify patterns in errors or target recurring classification issues. MPD's Risk Management Division, which is tasked with identifying, assessing, and mitigating organizational risks, confirmed it has not conducted recent risk assessments specific to crime classification or reporting accuracy, and no formal unit exists to maintain classification standards across the Department.

One incident documented during this inspection illustrates how, in the absence of a systematic review function, detection of classification issues can depend on individual initiative. In August 2025, an Office of Unified Communications dispatcher sought clarification after an MPD supervisor—under the impression that three separate calls were related to a single event—directed that they be recorded under one central complaint number (CCN). It was later found that the calls concerned three distinct burglaries occurring in close proximity. After the matter was elevated, the incidents were recorded correctly. Staff noted that situations of this kind are uncommon; this example is provided to show how, without a centralized review mechanism, identification of anomalies can rely on chance and the judgment of individual personnel rather than effectively designed controls.

Several personnel also reported that classification changes to submitted reports can occur without the reporting officer's knowledge. Patrol members described the in-system alert mechanism for modifications as insufficient and noted it has no email counterpart. A centralized review function with rejection authority and decision documentation requirements would create an auditable record of classification changes, the process by which they were made, and the decision rationale; no such process currently exists.[29]

MPD Reported Efforts to Reestablish a Centralized Review Function

MPD leadership has acknowledged the need to restore an independent report review function and has begun taking steps to do so. During this inspection, staff described ongoing efforts to reestablish a centralized unit under the Analytics Division with a focus on ensuring accurate classification of District offenses. MPD has developed position descriptions for dedicated staff who would perform this role, reflecting a clearer understanding of the expertise and capacity such a unit will require. Staff involved in the planning process emphasized that a revived review function should have defined access permissions within Mark43, the authority to return reports for correction, and a clear scope of review.

---

[29] *See* GAO Green Book, §§ 10.04, 12.02, and 16.09, which require organizations to document control activities, maintain written policies and procedures, and document the results of monitoring to identify internal control issues.

At the time of this inspection, these efforts were still underway. A finalized standard operating procedure had not yet been issued, staff had not yet been assigned, and a formal implementation timeline had not been established. Work in progress included developing internal processes, reviewing RMS role permissions, and assessing user-role configurations. To achieve the intended quality-assurance benefits, the revived function will need documented procedures, defined staffing, appropriate system access controls, and a regular reporting cadence to command leadership. Equally important, it will need to be embedded within a broader governance structure—one that includes updated policy, defined training standards, and proactive risk oversight—to ensure that the conditions that arose after the SRU's dissolution and went unaddressed for more than a decade do not recur.[30]

Recommendation 1

We recommend that the Chief, MPD:

Implement a permanent, independent review function to ensure accurate crime classification, detect potential crime reporting errors, and strengthen supervisory oversight. At a minimum, MPD should ensure this function:

A) has formalized authority, scope, and responsibilities through documented policies and procedures;

B) has enough dedicated personnel with appropriate training and system permissions, including the ability to return reports to officers for correction;

C) evaluates incident reports and calls for service to identify discrepancies that may indicate misclassification or reporting errors; and

D) implements structured reporting mechanisms, including regular management reports on classification accuracy, rejection trends, and identified discrepancies.

[30] *See* GAO Green Book, §§ 3.02–3.05, which require management to establish an organizational structure, assign responsibility, and delegate authority in a manner that supports effective internal control, including defining roles, reporting lines, and governance mechanisms needed for controls to operate as intended.

Management Response:

MPD agreed with our recommendation. MPD stated that in March 2026 it began establishing an internal function, independent of operational units, to continuously audit and evaluate police reports. To that end, MPD is consolidating its data management functions into a new Office of Data Integrity and Analytics within the Executive Office of the Chief of Police, composed of an Analytical Services Division and a Data Integrity Division. Within the Data Integrity Division, a new Data Quality and Compliance Branch will direct internal quality control, comprehensive report auditing, and continuous cross-checking for compliance with policy and the criminal code, and a renamed Federal Compliance Reporting Branch will continue to manage NIBRS compliance.

MPD reported that, in April 2026, it detailed NIBRS reporting quality control personnel to the Analytical Services Division and began recruiting dedicated sworn and professional personnel for the Data Quality and Compliance Branch. The Metropolitan Police Academy has prepared a four-day training course for sworn personnel assigned to the division and a two-week course for professional staff. MPD is developing tracking mechanisms, including dashboards and automated reports, to continuously validate data quality, including monitoring rejected reports, common errors, and the personnel most frequently associated with those errors. MPD anticipates that sergeants and officers will complete training and begin reviewing reports by mid-to-late August 2026, and that the function will be fully operational by the beginning of the new year.

MPD stated that its plans do not currently include analyzing or auditing calls for service data maintained by the Office of Unified Communications (OUC). MPD explained that calls to 911 and 311 are not classified under DC Code, that OUC operators are not trained in DC Code classification, and that differences between an operator's initial classification and the classification assigned following an officer's on-scene investigation are to be expected.

OIG Note:

We consider MPD's planned actions responsive to elements A, B, and D of this recommendation, and partially responsive to element C.

Our recommendation does not contemplate treating OUC's initial call assessment as offense classification, and we do not suggest that variance between an operator's categorization of a call for service and the subsequent crime classification denotes an error. Recognizing that there is not a one-to-one relationship between calls received by OUC and the resulting MPD crime reports, our intent is to ensure that MPD's quality-control mechanisms account for the continuum of risks across the entire crime data reporting process. These risks include identifying instances in which an incident entered in the Mark43 RMS is improperly modified, as well as instances in which calls for service are underreported in, or omitted from, resulting crime reporting—such as the situation illustrated in the August 2025 matter described in Finding 1. Evaluating OUC calls against crime reports in Mark43 can provide additional information relevant to both the accuracy and completeness of crime data.

Accordingly, we recommend that MPD reconsider incorporating a periodic comparison of calls for service received by OUC and resulting incident reports into the scope of the Data Quality and Compliance Branch.

Finding 2: MPD Lacked Effective System Controls over its Records Management System (RMS)

The absence of an independent classification review function was compounded by inadequate system controls within MPD's RMS. Mark43, MPD's current RMS, lacked both the technical controls to enforce basic reporting standards and the governed access structure necessary to protect data integrity.

MPD's policies establish clear expectations for narrative quality in incident reports. General Order 401.01 (GO-SPT-401.01), *Field Reporting System*, requires officers to produce organized, factual, and objective narratives, and MPD's Training Academy reinforces these standards, emphasizing that well written-reports are critical to prosecutorial decisions, civil litigation, and public accountability.[31] These standards recognize that the narrative is not incidental; it is the factual foundation for subsequent classification and investigative decisions. As part of this inspection, we evaluated MPD's RMS practices against the GAO Green Book, the federal criteria for determining whether internal controls are appropriately designed, implemented, and operating effectively.

[31] MPD, Curriculum Block 3: Report Writing, at 2, https://mpdc.dc.gov/node/1646701 (last visited May 8, 2026).

The inspection found that Mark43 does not ensure narrative standards at the point-of-entry. Officers can submit reports for supervisory review without completing narrative fields or meeting any threshold for sufficiency. No system warning or denial prevents incomplete reports from advancing up the chain of command. As a result, identifying deficiencies, such as blank data fields, relies entirely on supervisors reviewing each report individually, often under the same workload constraints that limit classification review.

Mark43 Does Not Enforce Narrative Requirements at Submission

A sample of 107 rejected reports which were initiated between 2021 and 2025 found that 66 (about 62 percent) were rejected by supervisors due to blank or insufficient narrative content or other missing required information. In each instance, Mark43 permitted the submission to reach the supervisory queue without flagging missing required content. This pattern is consistent with what supervisors and patrol members described: when the system does not enforce basic requirements at submission, narrative completeness and consistency vary significantly across officers and shifts.

Mark43 also allows for the feedback portion of a rejected report to be blank. When a report is rejected, officers primarily receive notice through an in-system alert—described by multiple officers as insufficient. Of the 107 rejected reports, 13 (approximately 12 percent) contained no supervisory notes explaining the reason for the rejection or required corrective action. Without clear feedback, officers may not understand what must be corrected or how to improve future submissions. The lack of documented rationales also prevents the accumulation of data needed to identify recurring error types or training needs.

User Permissions Were Not Documented or Aligned to Operational Roles

Mark43's user permissions are structured around assigned roles that combine operational rank with functional responsibilities to determine what each user can access and do within the system. This is a standard configuration for an RMS, but it requires clear documentation and ongoing governance to function as an effective control.[32] MPD maintained user accounts and knew who held them but had no documented framework specifying which permissions corresponded to defined responsibilities, nor a formal process governing how access is changed or reviewed.[33] Without that framework, personnel had limited visibility into what

---

32 *See* GAO Green Book § 12.03, which requires management to document, through policies and procedures, each unit's responsibilities, related risks, and control activities. Documentation must be sufficient to allow controls to be understood, monitored, and executed consistently across personnel.

33 *See* GAO Green Book § 11.11, which requires management to design logical access control activities that restrict system access to authorized users, limit permissions to functions commensurate with assigned responsibilities, and promptly update access rights when personnel change roles. These controls help prevent inappropriate access and unauthorized system changes.

access other personnel held, making it difficult to identify inappropriate access or detect unexpected changes.

Mark43's edit capability allows authorized users to modify approved report content, including offense classifications and case notes, without triggering a secondary approval step or notifying the reporting officer or their supervisor. This type of capability serves a legitimate purpose; in practice, it is used to correct data elements for federal reporting requirements. However, without a documented permission framework, routine audit log review, or automatic notifications to affected personnel, the same capability allows substantive changes to be made invisibly—creating a control weakness that is difficult to detect and nearly impossible to monitor systematically.

Lifecycle and Audit Controls Were Not Consistently Applied

Mark43's lifecycle and audit controls were also inconsistently applied. MPD did not have a formal account lifecycle process to ensure that permissions are reviewed and adjusted when personnel changes occur.[34] Remediation work, such as an automated inactive account protocol, was underway but not yet fully implemented during this inspection. While Mark43 records who accesses and edits reports, no unit was responsible for routinely reviewing those audit logs for data integrity purposes.[35] Staff described an environment where RMS practices relied heavily on individual expertise rather than documented, repeatable processes.

Taken together, the absence of point-of-entry safeguards preventing incomplete reports from advancing, the lack of a documented permission framework, the presence of edit capabilities without notification or routine oversight, and the absence of a formal account lifecycle process and audit log review weakened multiple layers of control simultaneously. These conditions are inconsistent with the internal control principles established in the GAO Green Book, which require agencies to design appropriate preventive and detective control activities, implement information technology controls that support data integrity, document roles and responsibilities, and conduct ongoing monitoring to ensure that controls operate as intended. Under these conditions, narrative quality and classification accuracy depend on individual judgment applied under time pressure rather than on designed, documented, and monitored controls.

---

[34] *See* GAO Green Book § 17.06, which requires management to complete and document corrective actions to remediate internal control deficiencies on a timely basis, including those associated with improper access, outdated permissions, or other system weaknesses identified through monitoring or evaluations.

[35] *See* GAO Green Book § 16.05, which requires management to perform ongoing monitoring of the design and operating effectiveness of internal controls as part of routine operations. Such monitoring activities include supervisory reviews, comparisons, reconciliations, data analytics, and other methods that detect control breakdowns or irregularities, including inappropriate system access or edits.

Recommendation 2
We recommend that the Chief, MPD: Establish and implement a formal access control framework for Mark43 that ensures user permissions are documented, assigned, and governed, subject to regular review and audit, and limited to authorized users performing their assigned duties.
Management Response: MPD agreed with our recommendation. MPD stated that in March 2026 it engaged Mark43 regarding the configuration of role-based access controls within the RMS and obtained a list of all active users, user roles, and permissions. MPD then initiated an audit of all internal and tenant users and purged inactive or redundant access to strengthen compliance with the FBI Criminal Justice Information Services Security Policy. In conjunction with the audit, MPD launched a revised internal online form requiring authorization justifications for initial or modified access to core systems and established internal business processes for timely and effective review of user accounts. Following the user audit, MPD reviewed role-based access controls and permissions, including record creation, viewing, editing, and deletion, and engaged Mark43 regarding attribute-based access control, enhanced report approvals, and notification systems. MPD stated that system configurations prevented the vendor from providing a swift resolution and that, to mitigate immediate risk, MPD implemented permission restrictions in April 2026 that would not interrupt operational workflows. A working group was subsequently formed to review and consolidate operational roles and to benchmark permissions against peer agencies, like the Boston Police Department. Following an on-site meeting in June 2026, MPD is awaiting final recommendations from the vendor for MPD's consideration.

Finding 3: Outdated Policies and the Lack of Proactive Risk Assessment Created Gaps in MPD's Crime Reporting Governance

MPD's governance of crime classification and reporting was undermined by two related conditions. First, many of the Department's policies describing how incidents are documented, classified, and reviewed have not been updated to reflect more than a decade of organizational and system changes. Second, MPD's Risk Management Division has never assessed risks related to crime reporting or classification accuracy. Together, these conditions mean that MPD's crime reporting environment is neither accurately documented in policy nor subject to the systematic oversight needed to identify where controls are absent, outdated, or ineffective.[36]

MPD's Governing Policies Were Outdated and Did Not Describe How Crime Reporting Works

MPD's policy framework for crime reporting was outdated, incomplete, and out of step with the Department's current structure and technology.[37] At the time of our inspection, the Policy and Standards Branch maintained a substantial backlog of directives requiring revision, and many directives central to crime reporting operations had not been updated in more than a decade. Rather than update or rescind prior directives, MPD issued new general orders when guidance changed. This practice created a patchwork of overlapping and sometimes conflicting policies, making it difficult for personnel to determine which requirements governed current operations, and normalized a culture of operating under outdated policies.

For example, the 2003 *Investigative Case Tracking and UCR Classification SOP* remained in effect even though it assigned dispute-resolution responsibilities to the Staff Review Unit (SRU),[38] which MPD disbanded in 2013. General Order 401.01, *Field Reporting System*, issued in 2012, also assigned responsibilities to the SRU, and it likewise remained in effect after the unit was dissolved.[39] As a result, both directives described responsibilities for an organizational component that no longer existed. Several additional directives still referenced systems and units that

---

36 *See* GAO Green Book § 16.01, which requires management to establish and operate monitoring activities to assess whether the internal control system is functioning as intended and to evaluate the results of those monitoring activities.

37 *See* GAO Green Book § 3.09, which requires management to develop and maintain documentation of its internal control system so that controls, responsibilities, and processes are clearly understood, communicated, and capable of being evaluated for effectiveness.

38 MPD, Investigative Case Tracking and UCR Classification Standard Operating Procedure (2003), II.H.5 at 17.

39 MPD General Order 401.01, Field Reporting System, Part VI.D at 22, (GO-SPT-401.01, effective July 19, 2012), https://go.mpdconline.com/GO/GO_401_01.pdf

MPD no longer used, including the Cobalt records system (which preceded Mark43) and the Morals Division (now defunct).[40]

Roughly one-third of MPD's general orders were more than 20 years old and had been overtaken by new technologies, updated RMSs, and changes to MPD's structure. As a result, personnel operated under policies that did not reflect current systems, structures, or expectations—creating operational ambiguity, normalizing policy noncompliance, and undermining both internal and external oversight.

MPD also did not maintain a current description of its end-to-end crime reporting process. No document showed how crime data flowed from initial entry through classification, review, approval, correction, and federal reporting. Without such documentation, the Department could not easily identify where controls existed, where controls were failing, or where new risks had emerged.

MPD's Risk Management Division (RMD) Has Never Assessed Risks Related to Crime Reporting Accuracy

The RMD's Operations Manual stated that its mission was to "proactively identify, assess, and mitigate potential risks." However, the Division had never evaluated risks related to crime classification, crime reporting accuracy, or data integrity, even after concerns about crime classification practices became the subject of external investigations. The RMD's audit cycle addressed a range of operational topics but never included crime reporting accuracy—an omission that is particularly significant given its implications for public transparency, federal reporting, and Department-wide accountability. The absence of risk assessment specific to crime reporting meant MPD lacked a structured mechanism to anticipate vulnerabilities and ensure controls were functioning as intended.[41]

MPD Lacks Enterprise-level Monitoring of Crime Reporting Accuracy

MPD did not maintain a centralized mechanism to track classification errors, reclassifications, or reporting trends across the Department. Although Mark43 generated audit logs that would have supported such monitoring, no unit reviewed them routinely to identify recurring errors or training needs. As a result, supervisors identified errors only through ad hoc individual reviews, and leadership lacked the information needed to detect systemic weaknesses in crime reporting.

The conditions identified in this finding reveal a governance structure that was outdated and not subject to routine, proactive oversight. The deficiencies identified

---

[40] MPD Executive Order 17-004, Cobalt: Booking Team Procedures (EO-17-004, effective date February 27, 2017), https://go.mpdconline.com/GO/EO_17_004.pdf; MPD, General Order 401.04, Reporting Violations of the ABC Regulations and License Law (GO-401.04, effective December 1, 1971), https://go.mpdconline.com/GO/GO_401_04.pdf; MPD personnel confirmed to OIG that all MPD orders posted online are active.

[41] *See* GAO Green Book § 7.02, which requires management to identify and analyze risks throughout the entity on both a periodic and ongoing basis as the foundation for designing and operating effective internal controls.

in Findings 1 and 2, including the lack of an independent review function and weaknesses in records management access controls, were not detected or corrected internally. Although MPD maintained processes for updating directives, it did not prioritize revisions based on operational or organizational risk, leaving outdated or inconsistent guidance in place for extended periods. Vulnerabilities of this type fall within the stated mission of MPD's Risk Management Division, which handles identifying, assessing, and escalating organizational risks; however, no recent assessments had examined risks associated with crime classification or crime reporting accuracy.

Recommendation 3
We recommend that the Chief, MPD: Ensure that all general orders, standard operating procedures, and other directives governing crime classification, records management, and federal reporting accurately reflect current organizational structures, authorities, and systems. Prioritize the 2003 UCR Classification SOP and General Order 401.01, Field Reporting System, and announce a timeline for completing these updates.
Management Response: MPD agreed with our recommendation. MPD stated that it is consolidating guidance regarding records management, crime classification, federal reporting, and the responsibilities and authority of the new Data Quality and Compliance Branch into an updated General Order 401.01, *Field Reporting System*. MPD stated that it plans to publish the updated order in coordination with the launch of the new branch.

Recommendation 4
We recommend that the Chief, MPD: Ensure that risks related to crime reporting accuracy and data integrity are systematically assessed on a recurring basis, with results reported to the Chief of Police as part of the Risk Management Division's regular audit cycle.
Management Response: MPD agreed with our recommendation. MPD stated that primary responsibility for ongoing audits of crime reporting accuracy and data integrity will be carried out daily by the Office of Data Integrity and Analytics, and that the Risk Management Division will conduct an annual audit of these processes beginning in fiscal year 2027.

Recommendation 5
We recommend that the Chief, MPD: Ensure that the Risk Management Division assesses the accuracy of MPD's governing policies annually.
Management Response: MPD agreed with our recommendation. MPD stated that the Risk Management Division routinely evaluates MPD policy during its audits and inspections and recommends updates when information is outdated or when it identifies areas for improvement. MPD stated that the Risk Management Division will publish an annual report of its policy-related recommendations.

Observation: MPD's Organizational Culture was Misaligned with its Published Values and Undermined its Crime Reporting Controls

We identified cultural conditions within MPD that weakened the Department's ability to maintain effective internal controls over crime classification and reporting. Personnel across multiple ranks and districts, sworn and civilian alike, consistently described an environment marked by limited trust, siloed communication, reluctance to raise concerns, and practices that did not align with MPD's stated mission and values. Although these conditions may not have caused the control failures documented in Findings 1–3, they contributed to them and help explain why those failures persisted and may continue without corrective action.

MPD's Observed Culture Did Not Align with its Published Mission and Values

MPD's Mission and Value Statement emphasizes transparency, accountability, employee support, and the expectation that every member can contribute to positive change.[42] Applied to crime reporting, these values reasonably require an environment in which personnel can raise concerns about classification errors, irregular practices, or supervisory influence without fear of reprisal.

[42] MPD, Mission of the Metropolitan Police Department, https://mpdc.dc.gov/node/132982 (last visited May 8, 2026).

Personnel described decision-making processes in which operational information was concentrated among a small group of individuals and not routinely shared with those responsible for implementing related policies or procedures. This environment limited personnel's ability to understand expectations, identify risks, or elevate concerns related to crime reporting. Interviewees also described instances in which supervisory personnel influenced crime classifications to align with anticipated or desired crime trends.

The absence of a protected internal reporting mechanism compounded these conditions. Personnel reported that MPD did not maintain a reliable means for employees to report suspected wrongdoing anonymously and without fear of reprisal; this is inconsistent with MPD's stated commitment to impartial investigation of misconduct and to empowering employees to influence positive change. Personnel who may have observed irregularities, but lacked a protected reporting channel, may not have felt comfortable reporting them, contributing to the ad hoc detection described in Finding 1.

The GAO Green Book identifies the Control Environment—leadership tone, modeled values, and internal information flow—as the foundation of an effective internal control system. Principle 1 requires a demonstrated commitment to integrity and ethical values, and Principle 14 requires internal communication of quality information. An environment in which personnel were reluctant to raise concerns, operational information was not routinely shared, and no protected reporting channel existed does not meet these principles. Should these cultural conditions persist, they will limit the effectiveness of structural improvements implemented in response to this report.

Sustained correction of the policy, governance, and access-control weaknesses identified in Findings 1–3 requires not only structural changes but an organizational environment in which those changes can take root.

Improvement Opportunity 1
MPD should align its organizational environment with the transparency and accountability values it has publicly committed to, with particular attention to the conditions that affect crime classification and reporting integrity.

Improvement Opportunity 2
MPD should pursue accreditation through an established, nationally recognized framework for law enforcement operations, including policy management, training, oversight, and reporting practices. Accreditation may provide MPD with a structured pathway to strengthen internal controls, modernize policy, and align crime data processes with professional standards.

CONCLUSION

Crime data is the informational foundation on which MPD makes operational decisions, the District allocates resources, and the public evaluates the safety of its communities. When that data cannot be relied upon, the consequences extend beyond inaccurate statistics: they affect officer deployment, legislative oversight, federal reporting, and the ability of residents and policymakers to hold MPD answerable for public safety.

The conditions documented in this report do not reflect isolated failures. They are the cumulative effect of a control framework that did not evolve commensurate with technological, operational, legal, regulatory, and societal changes.

We acknowledge MPD's initial steps to address some of these deficiencies. But the scale and duration of the deficiencies documented here will require more than incremental correction. Fully implementing these recommendations is MPD's clearest path to providing accurate, transparent, and reliable crime information to the District.

APPENDIX 1. FINDINGS

Table of Findings

No.	Finding
1	MPD Lacked a Cohesive Internal Control Framework for Crime Classification and Reporting
2	MPD Lacked Effective System Controls over its Records Management System (RMS)
3	Outdated Policies and the Lack of Proactive Risk Assessment Created Gaps in MPD's Crime Reporting Governance

APPENDIX 2. RECOMMENDATIONS

Table of Recommendations

Agency	No.	Recommendation	Status	Action Required	Finding
MPD	1	Implement a permanent, independent review function to ensure accurate crime classification, detect potential crime reporting errors, and strengthen supervisory oversight. At a minimum, MPD should ensure this function: A) has formalized authority, scope, and responsibilities through documented policies and procedures; B) has a sufficient number of dedicated personnel with appropriate training and system permissions, including the ability to return reports to officers for correction; C) evaluates incident reports and calls for service to identify discrepancies that may indicate misclassification or reporting errors; and D) implements structured reporting mechanisms, including regular management reports on classification accuracy, rejection trends, and identified discrepancies.	Open	Tracking implementation	1
MPD	2	Establish and implement a formal access control framework for Mark43 that ensures user permissions are documented, assigned, and governed, subject to regular review and audit, and limited to authorized users performing their assigned duties.	Open	Tracking implementation	2
MPD	3	Ensure that all general orders, standard operating procedures, and other directives governing crime classification, records management, and federal reporting accurately reflect current organizational structures, authorities, and systems. Prioritize the 2003 UCR Classification SOP and General Order 401.01, Field Reporting System, and announce a timeline for completing these updates.	Open	Tracking implementation	3
MPD	4	Ensure that risks related to crime reporting accuracy and data integrity are systematically assessed on a recurring basis, with results reported to the Chief of Police as part of the Risk Management Division's regular audit cycle.	Open	Tracking implementation	3
MPD	5	Ensure that the Risk Management Division assesses the accuracy of MPD's governing policies annually.	Open	Tracking implementation	3

APPENDIX 3. MANAGEMENT RESPONSE

GOVERNMENT OF THE DISTRICT OF COLUMBIA
METROPOLITAN POLICE DEPARTMENT

July 23, 2026

Matthew Wilcoxson
Interim Inspector General
Office of the Inspector General
100 M Street, SE, Suite 1000
Washington, DC 20003

Dear Mr. Wilcoxson:

Thank you for the opportunity to review and provide comment on the draft Inspection report, "The Metropolitan Police Department's Crime Data Reporting Processes and Data Reliability Controls." Overall, these recommendations are well aligned with steps that we have already begun to address the findings of this inspection and the internal investigation of the Metropolitan Police Department (MPD). Detailed responses to the recommendations are below.

Recommendation 1
We recommend that the Chief, MPD: Implement a permanent, independent review function to ensure accurate crime classification, detect potential crime reporting errors, and strengthen supervisory oversight. At a minimum, MPD should ensure this function: A) has formalized authority, scope, and responsibilities through documented policies and procedures; B) has a sufficient number of dedicated personnel with appropriate training and system permissions, including the ability to return reports to officers for correction; C) evaluates incident reports and calls for service to identify discrepancies that may indicate misclassification or reporting errors; and D) implements structured reporting mechanisms, including regular management reports on classification accuracy, rejection trends, and identified discrepancies.

Agree. In March 2026, MPD initiated the steps to establish an internal system independent of operational functions for continuously auditing and evaluating police reports. The objective is to obtain strict accountability across the department.

To achieve this goal, data management functions within MPD are being consolidated through the creation of the Office of Data Integrity and Analytics under the Executive Office of the Chief of

Police (EOCOP). Establishing this dedicated office is essential to eliminate departmental silos, enforce reporting objectivity, conduct systematic reviews of police reports, and uphold the agency's commitment to public transparency.

The Office of Data Integrity and Analytics will consist of two divisions: Analytical Services Division and Data Integrity Division. While the Analytical Services Division will maintain its existing responsibilities, data oversight will be managed through the Data Integrity Division, holding overall accountability for agency-wide data quality and compliance standards. Within that division, the Data Quality and Compliance Branch will direct internal quality control, comprehensive report auditing, and continuous cross-checking to ensure universal compliance with policy and criminal code. The renamed Federal Compliance Reporting Branch will continue to manage the agency's strict adherence to FBI National Incident-Based Reporting System (NIBRS) standards.

This restructuring is underway. In April 2026, the current NIBRS reporting quality control personnel were detailed to the Analytical Services Division from the Technical Services Bureau. At the same time, MPD began recruiting dedicated sworn and professional personnel for the Data Quality and Compliance Branch. This hiring process is underway.

The Metropolitan Police Academy has prepared a comprehensive four-day training for sworn personnel assigned to the division. Professional staff will receive a two-week course through the academy. Various tracking mechanisms are being developed to continuously monitor data quality. These tools such as dashboards and automated reports will track rejected reports, common errors, and the personnel most frequently involved in these errors.

We are developing our standard operating procedures with the goal of being fully operational by the new year. Parts of the work will begin as the units are stood up and personnel are hired. We anticipate sergeants and officers to complete training and begin to check reports by mid-to-end August. Upon onboarding and training additional personnel, we will broaden our scope and enhance our analytical focus. Getting these systems running smoothly is our top priority before we begin expanding our operations.

Please note, however, that plans do not currently include analyzing and auditing calls for service data from the Office of Unified Communication (OUC). As an initial matter, calls to 911 or 311 are not classified under DC Code, nor are the OUC operators trained on DC Code. Calls are classified under broad categories. Thus, changes between the initial classification by an operator based on a brief phone call and the eventual classification following an on-scene investigation by a police officer are to be expected. Beginning an analysis with the call classification would not be practical or useful.

Recommendation 2
We recommend that the Chief, MPD: Establish and implement a formal access control framework for Mark43 that ensures user permissions are documented, assigned, and governed, subject to regular review and audit, and limited to authorized users performing their assigned duties.

Agree. In March 2026, MPD engaged with Mark 43 to discuss the configuration of role-based access controls within the records management system (RMS). In response to our request, Mark 43, a multi-tenant RMS, provided a list of all active users, user roles, and permissions within the system.

Upon review of the data, MPD initiated an audit of all internal and tenant users. To bolster compliance with FBI Criminal Justice Information Services Security Policy, MPD successfully purged inactive or redundant access. In conjunction with this audit, MPD launched a revised internal online form to request initial or modified access to MPD core systems, modernizing internal access controls with strict authorization justifications. Internal business processes have been established for timely and effective review of user accounts.

Upon completion of the user audit, MPD reviewed role-based access controls and permissions such as record creation, viewing, editing, and deletion. MPD engaged with Mark 43 to evaluate immediate solutions to include attribute-based access control, enhanced report approvals and notification systems. Due to system configurations, Mark 43 was unable to provide swift resolution. To mitigate immediate risk, in April 2026, MPD implemented immediate permission restrictions that would not interrupt operational workflows. Subsequently, a working group was formed to review and consolidate operational roles, benchmarking permissions against peer agencies like the Boston Police Department. Following the most recent on-site meeting in June, the group is awaiting final recommendations from the vendor for consideration.

A successful framework rollout requires deep collaboration between MPD and Mark43. MPD has engaged the vendor for onsite support to streamline this process, ensuring accurate training materials, optimized modules, and seamless system functionality.

Recommendation 3
We recommend that the Chief, MPD: Ensure that all general orders, standard operating procedures, and other directives governing crime classification, records management, and federal reporting accurately reflect current organizational structures, authorities, and systems. Prioritize the 2003 UCR Classification SOP and General Order 401.01, Field Reporting System, and announce a timeline for completing these updates.

Agree. MPD is consolidating guidance regarding records management, crime classification, federal reporting, and the responsibilities and authority of the new Data Quality and Compliance Branch into an updated General Order 401.01 (Field Reporting). MPD is planning to publish the updated order in coordination with the launch of the new Branch as outlined above.

Recommendation 4
We recommend that the Chief, MPD: Ensure that risks related to crime reporting accuracy and data integrity are systematically assessed on a recurring basis, with results reported to the Chief of Police as part of the Risk Management Division's regular audit cycle.

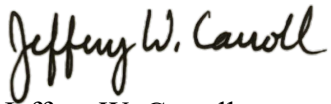
Agree. The primary responsibility for ongoing audits of crime reporting accuracy and data integrity will be carried out daily by the Office of Data Integrity and Analytics. In addition, MPD's Risk Management Division (RMD) will conduct an annual audit of these processes beginning in fiscal year 2027.

Recommendation 5
We recommend that the Chief, MPD: Ensure that the Risk Management Division assesses the accuracy of MPD's governing policies annually.

Agree. MPD's RMD routinely evaluates MPD policy when conducting their audits and inspections, and they provide recommendations for policy updates when information is outdated or when they identify areas for improvement. RMD will publish an annual report of their policy-related recommendations,

Work is well underway to establish a comprehensive program for data integrity and transparency. Our alignment with the OIG's recommendations suggests we are headed in the right direction. Please do not hesitate to contact me if you have any further questions.

Sincerely,



Jeffery W. Carroll
Interim Chief of Police

cc: Muriel Bowser, Mayor
Lindsey Appiah, Deputy Mayor for Public Safety and Justice

REPORT WASTE, FRAUD, ABUSE, AND MISMANAGEMENT

(202) 724-TIPS (8477) and (800) 521-1639

https://oig.dc.gov

oig@dc.gov

STAY UP TO DATE

instagram.com/OIGDC

x.com/OIGDC

facebook.com/OIGDC

Sign-up for email/text updates from OIG