

OFFICE OF THE INSPECTOR GENERAL

CITY OF BALTIMORE



Isabel Mercedes Cumming

Inspector General

Investigative Report Synopsis

OIG Case # 27-0002-I

Issued: September 9, 2026



OFFICE OF THE INSPECTOR GENERAL
Isabel Mercedes Cumming, Inspector General
City Hall, Suite 635
100 N. Holliday Street
Baltimore, MD 21202



September 9, 2026

Dear Citizens of Baltimore City,

The mission of the Office of the Inspector General (OIG) is to promote accountability, efficiency, and integrity in City government, as well as to independently investigate complaints of fraud, financial waste, and abuse. The following synopsis is a condensed version of the full report provided to City management officials and does not contain all investigative information.

This public synopsis provides information the OIG discovered during an investigation involving a senior City employee (Senior Employee). This investigation was the result of two earlier investigations of the same Senior Employee that began 2025. While the initial investigation was ongoing, the Senior Employee directed a BCIT Official (BCIT Official), to remove the OIG's Assistant Inspector General of IT's (AIG IT) permissions to access their email communications and documents. The AIG IT was an authorized user per established policies with permissions approved annually by BCIT.

This action would have interfered with an ongoing OIG investigation, impacting the City's Technology Acceptable Use Policy (Technology Policy) found in the City's Administrative Manual (AM). The Senior Employee halted the order to remove access only when they learned the AIG IT's authorized permissions allowed the AIG IT to regain access. This OIG report with concerns of potential abuse of power and prestige of office violations was provided to City leadership on July 20, 2026.

The Senior Employee's directive and actions occurred in November 2025, before Baltimore City Solicitor Ebony Thompson (Solicitor) published her legal analysis regarding the removal of the OIG's direct access on February 6, 2026.

BACKGROUND

Earlier Concern from City Leadership

Chief Administrative Officer Faith Leach (CAO) contacted the AIG IT directly in late June 2025 regarding the AIG IT's name being listed as an administrator to her electronic records. The AIG IT informed CAO that their permissions were left due to inadequacies in Microsoft 365's eDiscovery process resulting from an investigation. The AIG IT explained the technical reasons that caused his permissions to remain. The AIG IT believed there was a gap in communication and then attempted to explain the data retrieval process in plain language to the CAO. The AIG IT then used the term "glitch" to describe the inadequacies and why his permissions were left behind after the data retrieval process.

The AIG IT suggested the CAO contact Inspector General Isabel Cumming (IG) directly. The CAO then emailed the IG and wrote that she was saving a "personnel" document and noticed the AIG IT was listed as an administrator on her document. The IG replied and wrote there was no error and it had been part of an investigation. The CAO then wrote that the hold was "concerning" given that the original document was a "pre-decisional budget document that I turned into a personnel document. Given the nature of my role and my access to privileged, deliberative documents, a broad base hold on all of my documents is concerning." Once

REPORT FRAUD, WASTE AND ABUSE

HOTLINE: 443-984-3476/800-417-0430 EMAIL: OIG@BALTIMORECITY.GOV WEBSITE: OIG.BALTIMORECITY.GOV

This public synopsis is only a summary of a more comprehensive report of investigation submitted to the appropriate City management official

the IG learned the AIG IT's permissions were still attached to the CAO's OneDrive, the IG asked the AIG IT to remove their permissions as the data retrieval process had been completed more than a month before. After speaking with the AIG IT, the IG used the AIG IT's words and wrote the technical "glitch" caused by the Microsoft 365 eDiscovery process had been rectified. This meant to the IG that the AIG IT had removed their permissions from CAO's OneDrive.

In the weeks following, the AIG IT also communicated with BCIT's InfoSec (security) team to confirm they could continue to monitor the AIG IT's activity.

City Policies & Notice

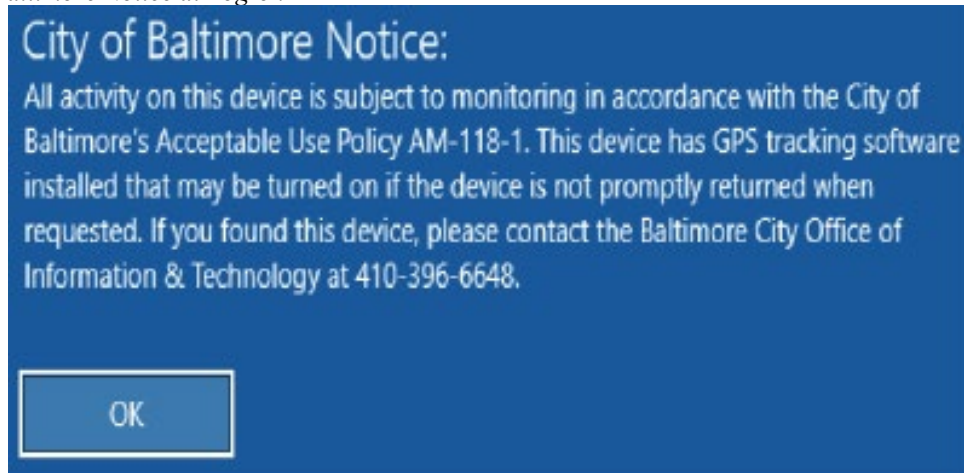
The Technology Policy provides the City's technology and property policies.¹ The Technology Policy clearly includes the Office of Inspector General as part of the oversight of those policies under the compliance section (AM 118-1 Part VII). The OIG has issued prior reports regarding City employee violations of the Technology Policy over the years. The policy includes the following statements:

- "Use of the City's computer and network resources is a privilege. The City expects users of the City's IT resources to act in a responsible, professional, ethical, and law-abiding manner."
- "Users may not engage in deliberate activity to degrade the performance of the City's IT resources, deprive an authorized user access to the City's IT resources, obtain extra City IT resources beyond those allocated, or circumvent the City's IT resources security measures."
- "As representatives of the City, users are responsible for all content created utilizing the City's IT resources including emails, texts, chats, audio, voice mail, faxes, images, whether digital or hard copy. Creating fraudulent, harassing, or sexually explicit content is prohibited. Content that may be inappropriate or offensive based on race, sex, religion, national origin, physical attributes, disabilities, sexual preferences, age, or other characteristics protected by law are prohibited. Users are required to report offensive content to their supervisors or Human Resources. Users shall not create or transmit content under an assumed name or attempt to obscure the origin of any content."
- "Users found in violation of this Technology Acceptable Use Policy are subject to disciplinary action up to and including restriction, possible loss of privileges, suspension, or termination. If necessary, the City will notify the City's Law Department, OIG, or law enforcement of any legal violations."
- "The City owns all rights to all content created, updated, or maintained on City IT resources unless ownership rights are reserved in writing to a third party or unless federal copyright or other laws provide for different rights. Users have no expectation of privacy when using City IT resources. The City reserves the right to access and monitor all messages, files, logs, and content created using City IT resources. Communications or content may be subject to disclosure to BCIT, the Office of Inspector General ("OIG"), the Law Department, law enforcement, or the Department of Human Resources ("DHR"), to the fullest extent allowed by law."

A notice is present when City employees log on to their computers, as shown in Figure 1 below. The notice explicitly states that "all activity on this device is subject to monitoring." A City employee, by clicking the "OK" button, expressly consents to the terms of the policy.

¹ Technology Policy: <https://codes.baltimorecity.gov/us/md/cities/baltimore/administrative-manual/100/AM-118-1>

Figure 1: City of Baltimore Notice at Log-on



Senior Employee Directive To Remove OIG Access

In early 2025, the OIG opened an investigation which concluded in 2026. As part of that investigation, the OIG reviewed the Senior Employee's correspondence. The correspondence revealed the Senior Employee and the BCIT Official discussed OIG access to records in November 2025. The exact correspondence ensued:

Nov. 2025 Time	Sender	Messages (Capitalization added & Positions inserted for Names)
11:45 a.m.	Senior Employee	• Take [AIG IT] off access to my sharepoint please • Its been months and no one is doing anything about it
11:49 a.m.	BCIT Official	• This is a sticky area. Traditionally in terms of OIG and permissions, we don't interfere with that. I'll request our staff to cut that, but so you're aware, I can't do that for others. People reach out to us seeing OIG is attached to their folders and we refer them to OIG.
11:52 a.m. to 11:53 a.m.	Senior Employee	• I am taking it up with the CA now • Its been months and there is no reason for this • And I would never ask you to do that for anyone • This overstep and overreach of her authority is too much and I am very willing to take this issue on
11:55 a.m.	BCIT Official	• Totally agree, so shall I hold off for now? I'm pretty sure once they attach to a person's drives they don't generally detach.

12:07 p.m.	Senior Employee	• Yes hold off
12:12 p.m.	Senior Employee	• Cut the access • If she requests it again, let me know and I will respond accordingly
12:58 p.m. (46 minutes later)	BCIT Official	• I'll request the access be cut. I believe [AIG IT's] rights are such that they won't need to ask us to restore it, [they'll] just do it [themselves]. Although he or she will ask us why it was cut
12:58 p.m. to 12:59 p.m.	Senior Employee	• Uuuggghhhhh • Well if that is the case then let me just address it with her

The BCIT Official's messages to the Senior Employee show that BCIT had knowledge of AIG IT's permissions and purpose for that access. The City's Technology Policy does not list the Senior Employee's agency as an authorized oversight or review agency for electronic communications.

The Senior Employee directed the BCIT Official to remove the OIG's access to their documents during an ongoing investigation. According to the correspondence, the Senior Employee only relented when they learned the AIG IT's level of access allowed the AIG IT to reattach their permissions. The Senior Employee's order to the BCIT Official would violate the City's Technology Policy, which states:

“Users may not engage in deliberate activity to degrade the performance of the City's IT resources, deprive an authorized user access to the City's IT resources, obtain extra City IT resources beyond those allocated, or circumvent the City's IT resources security measures.”

The Senior Employee's order to remove the AIG IT's permissions could also be a prestige of office concern. According to the City's Ethics Law, “a public servant may not intentionally use the prestige of his or her office or position for his or her own private gain or that of another.”

Within 90 minutes, the Senior Employee wrote to the IG, “It has come to my attention that your office has and continues to maintain access to my email and shared drive—both in my prior capacity [job title removed] and in my current capacity as [job title removed]. Is there some reason or purpose for this unfettered access? I would greatly appreciate your response.”²

The IG replied that “the information concerns ongoing confidential investigations that the OIG is undertaking

² The use of the words “unfettered access” should be noted as this was the first mention to the OIG of that term and the wording also appeared in the BCIT and Law Department press release on January 24, 2026. This term continues to be used by City leadership (as seen in the City's response to this report), which is not accurate. The OIG has always had direct access with BCIT's knowledge as shown by the BCIT Official's replies to the Senior Employee.

per our Charter responsibilities. As described in AM 118-1, limited departments can conduct such investigations per their respective mandates. The [Name of City Agency removed] nor the [Name of City Agency removed] fall within those parameters. My current concern is how you became aware of this confidential information as it can impact other ongoing investigations. Please advise.”

The Senior Employee wrote back to the IG, asserting that “I am not under any investigation nor am I party to one.” IG Cumming notified the Senior Employee that, “[a]s the OIG informed you in a previous investigation, there is no notice given for any investigations in either local or federal cases. The only notice ever provided is for audits which the OIG does not do. You are part of an ongoing confidential investigation. We plan on interviewing you next week. Again, please advise as to how you became aware of any technology access.” The Senior Employee did not respond to how they became aware of the technology access to emails or documents.

In a later email review, after the OIG interview, the Senior Employee wrote the following to a Quasi-City Agency Leader: “You know Isabel reads all my shit because she thinks its legal for her to have unfettered access. I won’t even go there on her lack of integrity.”

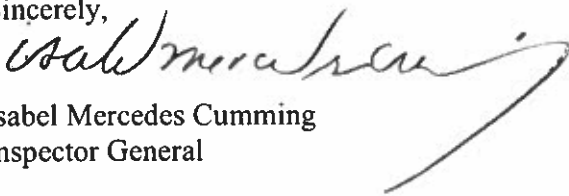
The Quasi-City Agency Leader replied, “My Lord! You really need to talk to Ebony [Solicitor]. That is ILLEGAL!”. The Senior Employee responded: “I have talked to Ebony [Solicitor]. I said I was going to sue her in my personal capacity because I’m not scared of her ass. AT ALL.”

FINDINGS

The Senior Employee’s order appears to engage in deliberate activity to deprive an authorized user’s legitimate access to the City’s IT resources. This directive is potentially a violation of the City’s Technology Policy. The Senior Employee rescinded the order when they learned that the AIG IT’s permissions could allow them to regain access to their correspondence and documents. The AIG IT’s permissions were long-established with BCIT’s approval.

The Senior Employee was not part of an enumerated agency per the Technology Policy and assumed the authority to order the OIG’s access to their City emails and documents be cut. This action could have limited the OIG’s access to documents that were relevant to ongoing investigations. Issuing the order to cut or limit access into an investigation in which they were a person of interest could represent a potential abuse of power and prestige of office concern.

Sincerely,



Isabel Mercedes Cumming
Inspector General

CC: Hon. Brandon M. Scott, Mayor of Baltimore City
Hon. Zeke Cohen, Baltimore City Council President
Hon. Bill Henry, Baltimore City Comptroller
Honorable Members of the Baltimore City Council