OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security
Washington, DC 20528 | www.oig.dhs.gov

March 2, 2026

BY ELECTRONIC TRANSMISSION

The Honorable Rand Paul
Chairman
Senate Committee on Homeland Security and Government Affairs

The Honorable Gary Peters
Ranking Member
Senate Committee on Homeland Security and Government Affairs

The Honorable Andrew Garbarino
Chairman
House Committee on Homeland Security

The Honorable Bennie Thompson
Ranking Member
House Committee on Homeland Security

The Honorable James Comer
Chairman
House Committee on Oversight and Government Reform

The Honorable Robert Garcia
Ranking Member
House Committee on Oversight and Government Reform

Re: Department of Homeland Security obstruction of OIG work

Dear Chairman Paul, Ranking Member Peters, Chairman Garbarino, Ranking Member Thompson, Chairman Comer, and Ranking Member Garcia:

Pursuant to Pub. L. No. 119-4,[1] I am writing to notify you that over the last several months the Department of Homeland Security (DHS or Department) has systematically obstructed the work of the DHS Office of Inspector General (OIG).

Background

OIG is authorized to conduct criminal investigations into allegations that have a nexus to DHS, as well as audits and inspections of DHS programs and operations.[2] The

[1] 139 Stat. 9; *see also* Joint Explanatory Statement for Department of Homeland Security Appropriations Act, 2024, Div. C, at 11-12. Although as a technical matter these authorities are no longer in effect, I have an inherent obligation to notify the relevant committees of Congress when DHS hinders OIG's work. If the committees consider these authorities to remain in effect, this letter satisfies OIG's reporting obligation for the first quarter of Fiscal Year 2026.

[2] 5 U.S.C. §§ 402(b)(1), 404(a).

Inspector General Act gives OIG a broad right of access to all DHS records and information in carrying out its work.[3]

There are only two exceptions to this right of access. First, the Department may limit or deny OIG's access to records or information when the records or information are covered by a "provision of law enacted by Congress that expressly – (i) refers to the Inspector General; and (ii) limits the right of access of the Inspector General."[4] Second, when an audit, inspection, or investigation involves national security, intelligence, counterintelligence, counterterrorism, or similar sensitive matters, the Secretary is empowered to limit OIG's access to records, or to terminate an OIG project altogether, "to prevent the disclosure of [classified or otherwise sensitive] information . . ., to preserve the national security, or to prevent a significant impairment to the interests of the United States."[5] However, if the Secretary were to exercise this power, she would be required to notify me in writing and state the reasons for her action. I would then be required to notify the President and Congress and state whether I agree or disagree with the Secretary's action.[6] I have never received a written notification from any DHS Secretary or Acting Secretary invoking this authority.

Apart from the Inspector General Act, longstanding principles of comity dictate that a federal agency should always cooperate in a federal criminal investigation. While individuals may assert personal privileges and rights under the Constitution and various statutes in connection with a criminal investigation, a federal agency has no institutional privileges or rights that would allow it to withhold government records from federal Criminal Investigators.[7]

Denial of access to records and information

Attachment A catalogues numerous OIG matters in which the Department has blocked OIG from accessing records and information necessary for OIG's work. While all of the matters listed are important, the Department's obstruction is particularly egregious in a specific pending criminal investigation. In early 2025, another federal law enforcement agency asked OIG to join an ongoing criminal investigation with national security implications that has a nexus to DHS. On April 3, 2025, OIG requested access to a database controlled by the DHS Office of Intelligence & Analysis (I&A) known as CI2MS, in connection with that criminal investigation. The Department proposed conditions on OIG's access that OIG cannot accept, because those conditions would require OIG to reveal details of the

[3] 5 U.S.C. § 406(a)(1)(A).

[4] 5 U.S.C. § 406(a)(1)(B).

[5] 5 U.S.C. § 417(a)(1), (2).

[6] 5 U.S.C. § 417(a)(3).

[7] *See In re Grand Jury Subpoena*, 112 F.3d 910 (8th Cir. 1997).

investigation to individuals who do not have a need to know, and who may be related somehow to the allegation(s) or individual(s) under investigation. The Department's proposed approach would risk compromising the investigation and needlessly complicate it and any potential prosecution by creating additional witnesses with knowledge of investigative steps and evidence gathered.

On December 19, 2025, I sent a letter to Secretary Noem asking for her assistance in resolving the access problems described in Attachment A.[8] Attachment B is a January 30, 2026 letter that DHS General Counsel James Percival sent to me in response to my letter to the Secretary.[9] Mr. Percival's letter indicates that the Department will not provide access to the requested records and information unless and until OIG provides additional justification for its requests under a manufactured and confusing framework involving "six distinct variables" that are not derived from the Inspector General Act.[10] Notably, Mr. Percival's letter does not cite a law enacted by Congress that expressly limits OIG's access to Department records or information. Moreover, the Secretary has not invoked her statutory authority to limit or deny OIG's access to Department records or information. As stated above, these are the only two potential legal justifications for DHS to block OIG's access.[11]

Two other aspects of Mr. Percival's letter warrant comment. First, contrary to the letter, OIG has not requested "continuous, unlimited, and real time access to all information systems of the Department at any time." Second, it is inappropriate for Mr. Percival to suggest that OIG is inclined to go on "fishing expeditions." It has been nearly seven years since the Senate, by unanimous consent, confirmed my nomination to be Inspector General of DHS. Since then I have established a track record of rigorous, *objective* oversight of DHS programs and operations, carried out according to applicable professional standards. It would be inefficient, not to mention an abuse of the authority granted to OIG by law, for OIG personnel to rummage through DHS records with no clear

[8] *See* 5 U.S.C. § 406(c)(2) (the Inspector General shall report to "the head of the establishment" when OIG's request for records or information is "unreasonably refused"); 5 U.S.C. § 401(3) (for purposes of section 406, at DHS the Secretary is the "head of the establishment").

[9] Mr. Percival's assistant asked that OIG provide his letter to Congress in the event that OIG notifies Congress of ongoing access problems.

[10] Consistent with the principles in the *Government Auditing Standards* (Government Accountability Office 2024) and the *Quality Standards for Inspection and Evaluation* (Council of the Inspectors General for Integrity & Efficiency 2020), at the outset of every audit, inspection, and evaluation, OIG notifies the relevant component of the Department in writing of the subject matter of the project, its scope, and its objective. It is unclear why Mr. Percival claims to need additional information to help him decide whether a particular OIG request for records and other materials should be granted or just what additional information OIG must provide to him before DHS complies with the OIG's request.

[11] The Secretary recently asked OIG to provide her with a list of all pending OIG matters, including criminal investigations, so that she may consider whether any audits, inspections, or investigations should be terminated under 5 U.S.C. § 417(a)(2).

purpose. It is far-fetched to think that I would suddenly sanction such conduct by the personnel in the office I lead.

OIG is experiencing additional access denials and delays, beyond those listed in Attachment A. Once the lapse in the DHS appropriation is cured, OIG will resume the resolution process with its counterparts in the Department. In due course OIG will report to Congress on any of these additional access denials that cannot be resolved.

Refusal to perform ministerial step to allow OIG personnel to have access to compartmented information outside of DHS

I&A, which is the conduit between DHS and the rest of the Intelligence Community (IC), typically conducts an indoctrination of DHS personnel into any compartmented intelligence program under the authority of the Director of National Intelligence after the IC agency that owns the data approves a request for access. This indoctrination is a purely ministerial step.

Following the attempted assassination of then-former President Trump on July 13, 2024, OIG opened a project aimed at assessing how the Secret Service identifies, receives, disseminates, and operationalizes intelligence concerning threats to protectees. Last year, an IC agency outside of DHS approved my request for access to a compartmented intelligence program administered by that agency, which contains information relevant to the OIG project. However, since September 2025, I&A has refused to conduct my indoctrination, thereby stymieing our work on this project. This is especially troubling given the other reported attempts on President Trump's life coupled with the present worldwide conflict.

Further, on November 3, 2025, another IC agency outside of DHS approved OIG personnel for access to a compartmented program administered by that agency so that our office can work a national security criminal investigation with another law enforcement agency. I&A has refused to conduct the indoctrination of OIG personnel.

I would be grateful for your support in resolving the problems described above. Should you have any questions, you may call me, or a member of your staff may contact OIG-CongressionalAffairs@oig.dhs.gov.

Sincerely,

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2026.03.02 10:17:03 -07'00'

Joseph V. Cuffari, Ph.D.
Inspector General

Attachments

ATTACHMENT A

UNCLASSIFIED/FOR COMMITTEE USE ONLY

SUMMARY OF INSTANCES OF UNREASONABLE DENIAL OF OIG REQUESTS FOR ACCESS TO DHS RECORDS AND INFORMATION

FEBRUARY 26, 2026

	DATE OF REQUEST	PROJECT NUMBER	DESCRIPTION
1	2015 (approx.)	various	OIG had access to ICE's Enforcement Integrated Database (EID) for approximately 10 years; EID data supported numerous OIG audits and inspections, and also facilitated OIG's risk analysis aimed at developing future OIG projects; on 11/19/25, acting at CBP's request, ICE revoked OIG's access
2	1/10/25	24-036-AUD-CBP	CBP refuses to give OIG personnel direct access to BorderStat, a data warehouse containing up-to-date information about border crossings, inspections, and related activities; without such access, OIG cannot independently assess completeness or reliability of data
3	4/3/25	I25-HSI-SID-21075	I&A is blocking OIG Criminal Investigators from accessing the Counterintelligence Information Management System (CI2MS) database, which they need for a criminal investigation with national security implications; I&A is refusing to honor the Department's 7/28/25 commitment to provide access upon the authorization of the Director of National Intelligence, which OIG obtained on 9/5/25
4	5/23/25	25-031-AUD-TSA	CBP will not allow OIG personnel access to the TECS relational database, which contains up-to-date data on CBP's border screening and admitting processes; OIG is unable to independently review data or conduct comprehensive risk analysis

Additional details and timelines of each delay and denial available upon request.

5	5/25	I25-HSI-SID-21075 & I24-CBP-SID-19662	On 9/29/25, DHS revoked OIG Criminal Investigators' standing access to the Integrated Security Management System (ISMS), a database containing detailed information about DHS employees and contractors who are eligible for access to classified information; such standing access allowed OIG to obtain crucial information needed in national security and otherwise sensitive investigations without making case-by-case requests for access, which create unnecessary delay and risk compromising an investigation by revealing subjects and related parties to those who do not have a need to know
6	7/18/25	24-051-AUD-TSA	TSA will not permit OIG to have direct access to the Secure Flight System database; this prevents OIG from conducting a comprehensive risk analysis; although TSA provided data extracts, OIG could not validate the information in the extracts
7	8/11/25	OIG risk assessments	CBP will not give OIG direct access to the Unified Immigration Portal, which contains data on CBP enforcement activity such as arrests, detentions, and releases; CBP will provide predefined extracts only, which prevents OIG from conducting real-time analytics to identify emerging risks and trends
8	9/5/25	25-020-ISP-I&A (& USSS)	I&A refuses to conduct the purely ministerial act of indoctrinating OIG personnel into a compartmented program; the data owner has authorized OIG's access; I&A's intransigence is impeding an OIG review related to the July 13, 2024 attempt to assassinate then-former President Donald Trump in Butler, PA
9	9/16/25	25-037-AUD-I&A	I&A is blocking OIG personnel from accessing the CI2MS database, which is needed for an audit of how I&A conducts counterintelligence investigations
10	9/24/25	25-038-AUD-ICE	ICE will not allow OIG to access its Integrated Decision Support system, thereby preventing OIG from conducting an independent, comprehensive review of data to support an audit

Additional details and timelines of each delay and denial available upon request.

11	10/24/25	I25-HSI-SID-21075	I&A refuses to conduct the purely ministerial act of indoctrinating OIG personnel into a compartmented program; the data owner has authorized OIG's access; I&A's intransigence is impeding a criminal investigation with national security implications

Additional details and timelines of each delay and denial available upon request.

ATTACHMENT B

Office of the General Counsel
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

January 30, 2026

VIA ELECTRONIC MAIL

Joseph Cuffari
Inspector General
Office of the Inspector General
Department of Homeland Security
Washington, DC 20528

Re: Office of the Inspector General (OIG) Access Requests

Dear Mr. Cuffari,

I write in response to your letter dated January 27, 2026, sent as follow up to our meeting on January 23, 2026. Since I was sworn in as General Counsel, I have been diligently engaging with you to help resolve whatever issues exist with your access to documents at the Department of Homeland Security. During those interactions, you have refused to provide answers to basic questions that would allow me to assist you. Now I understand that you are threatening to send a letter to Congress to report that the Department is preventing you from obtaining access to records. I want to be clear, as I have been clear in all our meetings, I cannot help you if you will not answer the basic questions I have posed to you. Given all that context, and the further context discussed below, I view any notification to Congress that you are being denied access to records as in bad faith and bordering on a material misrepresentation to Congress.

I will start at the beginning. You sent a letter to the Secretary dated December 19, 2025, the same day I was confirmed as General Counsel, demanding access to records and information. As you know, however, confirmation is not the last step—a person must be subsequently appointed by the President before that person assumes office. That did not occur until December 21. You also did not actually send the letter to me. In other words, you listed "James Percival, General Counsel" on the CC line of your letter even though I was not the General Counsel and even though you did not actually provide a copy to me as your letter indicated. The first time I heard from you on this matter was January 12, 2026, when you finally emailed me the December 19 letter and asserted that you planned to notify Congress in six days that your information access requests had not been resolved within 30 days of the December 19 letter.

We met shortly thereafter in person for an introductory meeting in my office on January 15, 2026. The meeting was initiated by me, and I made clear that I wanted you to have all access that you are legally entitled to. You did not dispute that the December 19 letter was never sent to me and agreed that it would be in the best interests of both the Department and OIG for us to work together first to resolve your information access requests before involving Congress. To that end, we scheduled a follow-up meeting on January 23, 2026, to discuss specifics about your information access requests.

During our January 23 meeting, you again agreed to work together amicably to resolve legal matters, and, in light of my recent confirmation as General Counsel, to hold off on going to Congress until

we had a chance to discuss and work through our respective legal positions. At the meeting, you repeatedly asserted that you were being denied access. I responded that in my mind, there were six distinct variables we needed to run to ground. First, I needed to know whether the problems were (a) delay, (b) outright refusal, or (c) disagreements about the scope of access needed for a particular matter. Second, I needed to know what your basis for access was for (a) audits as compared to (b) criminal matters, which each might present different legal frameworks. At the end of the meeting, I requested that you explain which bucket each instance fell into and provide a short legal explanation for the authorities governing access in each circumstance.

January 23 was a Friday. In the days following, you were aware or should have been aware that I was working in person at FEMA protecting the American public from a deadly snow and ice storm that closed the government for several days. Yet, instead of doing what we agreed on, you sent a "follow up" letter on Tuesday, January 27 lacking any of the information I requested and again threatening to immediately go to Congress. January 27 was the Tuesday after our meeting, which means your "follow up" letter occurred without the government being open a single day between our meeting and that letter. Despite this timing and the surrounding circumstances, the letter included a threat to "notify committees of jurisdiction" that "the Department delays fulfilling or outright denies an OIG request for access to Department records." As discussed, this statement was disingenuous because you never responded to my reasonable request for information so that I could adjudicate the alleged issues.

While I continue to believe that you providing the requested information is the best path forward, below is my tentative understanding of the current issues. As I best understand, you have refused to engage in a scoping process and instead demand unfettered access to every system in the Department. I do not believe you are legally entitled to that level of access. In fact, I believe providing you that access would be unlawful.

OIG Must Communicate to Department Management the Scope of Information Access Requests for Audits and Investigations

Your position that OIG should have unfettered access to all Department records and information systems for audit and investigations purposes is not supported by law. The Inspector General Act allows the Inspector General to access records "which relate to the programs and operations with respect to which that Inspector General has responsibilities." 5 U.S.C. § 406(a)(1)(A). Thus, the Inspector General does not have unlimited access to Department records and may only access the subset of records that relate to his specific oversight responsibilities.

The Inspector General Act further mandates that the Inspector General comply with the Government Accountability Office "Yellow Book" Auditing Standards. 5 U.S.C. § 404(b)(1)(A). These standards impose rigorous professional requirements that limit fishing expeditions and preserve the distinction between auditor and management. Auditors must document an audit plan that has a nexus to the audit objectives. Yellow Book, Sec. 8.03. The plan must explain the scope of the audit and identify the documents necessary to carry out the audit: "*Scope is the boundary of the audit* and is directly tied to the audit objectives. The scope defines the subject matter that the auditors will assess and report on, such as a particular program or aspect of a program, *the necessary documents or records*, the period of time reviewed, and the locations that will be included." *Id.*, Sec. 8.10 (emphasis added). Importantly, auditors must "communicate an overview of the objectives, scope, and methodology and the timing" of the audit to management. *Id.*, Sec. 8.20.

Thus, the Inspector General must document the scope of its audit plan, identify the documents it seeks as part of the plan, and communicate the scope of the audit plan to Department management. Your request for continuous, unlimited, and real time access to all information systems of the Department at any

time you want is not allowed under the Inspector General Act. It is so grossly overbroad as to subsume and "tak[e] on the role of management or otherwise perform[] management functions on behalf of the audited entity," a concern called out in the Yellow Book as the "management participation threat" with a warning to auditors to avoid this practice. *Id.*, Sec. 3.30(f).

Audits and Investigations on Classified Information Systems are Subject to the Same Scoping Requirements

Audits and investigations conducted on classified information systems are subject to the same scoping requirements explained above, except that this approach is even more warranted. The Inspector General Act makes no distinction in the conduct of audits and investigations on classified versus unclassified systems, but I am concerned that your push for unfettered access to classified information in the Department's possession would violate the longstanding principle of need-to-know. Regardless of an individual's position, Executive Order 13526 and Intelligence Community policies make clear that access to classified systems is granted on a need-to-know basis, and individuals may access classified information only if they are favorably determined eligible for access and have signed a nondisclosure agreement. *See* Exec. Order No. 13.526, § 4.2(a)(1)-(3). These rules make no distinction whether access is for criminal, civil, or audit purposes.

I am also concerned about representations you made to my predecessor, the Acting General Counsel, and reiterated again during our January 15 introduction meeting, that all inspectors general in the intelligence community have unfettered access to classified systems at their respective intelligence agencies. This office checked on that claim and it appears to be inaccurate.

Furthermore, some of this classified information originates with other agencies in the intelligence community, as marked with originator control, and the Department must obtain advance permission from the originating agency before extending access beyond the originally authorized recipients. *See* Intelligence Community Directive (ICD) 710, *Classification Management and Control System* (Jun. 21, 2013), § D.1.e.; *see also generally* Intelligence Community Policy Guidance (ICPG) 710.1, *Application of Dissemination Controls: Originator Control* (Jul. 25, 2012). Even when such access is granted, recipients generally may not take investigative, operational, or legal action based on originator control material without the originator's (and in some cases the Attorney General's) prior approval. ICPG 710.1, at E.2. These originator-control requirements make unfettered, system-wide access to the Department's classified intelligence systems impractical and inconsistent with our government-wide obligations.

Finally, the Inspector General Act provides that for certain sensitive audits and investigations involving intelligence, counterintelligence, counterterrorism, or confidential sources, the Inspector General operates under the authority, direction, and control of the Secretary, who may prohibit specific audits, investigations, or access to information when necessary to prevent disclosure that would harm national security or significantly impair U.S. interests. 5 U.S.C. § 417. Allowing the Inspector General permanent, unscoped access to all the Department's systems or records would effectively bypass these protections and strip the Secretary of her statutory authority over sensitive disclosures.

The Criminal Nature of an Investigation Does Not Change the Scoping Requirements

To the extent you assert that the criminal nature of an investigation transforms the Inspector General's access rights, it does not. The Inspector General Act itself does not contemplate a difference in the conduct of an investigation when it is performed for civil, criminal, or administrative purposes. The Inspector General must abide by the same scoping requirements to tie the documents sought to the documented scope of the investigation. This is especially true when seeking access to sensitive information concerning "ongoing criminal investigations and proceedings," which the Inspector General Act expressly

places under the Secretary's authority, direction, and control. 5 U.S.C. § 417(a)(1)(B).

* * *

As I have said repeatedly, I prefer to work together to resolve your information access requests. Please provide me with the lists of information requests categorized into the buckets outlined above, plus your counsel's legal explanation for the authorities governing access in each circumstance.

Sincerely,

James H. Percival II
General Counsel