

Office of Inspector General
Internal Investigations Unit (IIU)


2026-06-05

Table of Contents

1950 Confidentiality of Investigative Information	1
Policy	1
Authority	1
References	2
Applicability	2
Definitions	2
Responsibility	2
History	2
Evaluation	2
1951 Authority and Responsibilities	3
Policy	3
Authority	4
References	4
Applicability	4
Definitions	5
Responsibility	5
History	5
Evaluation	5
1952 Retention of Investigative Records	6
Policy	6
Authority	7
References	7
Applicability	7
Definitions	7
Responsibilities	7
History	7
Evaluation	7
1953 Workplace Violence - External Threats	8
Policy	8
Scope	8
Definitions	8
References	10
General Provisions	10
Warning Signs	10
Establishing a Plan	11
Reporting of Acts or Threatened Acts of Violence (External Source)	11
Handling of External Customers	12
Staff Training Requirements	12

History	12
Evaluation	13

1950 Confidentiality of Investigative Information

	Department of Human Services Policy and Manual Management System	Index: POL 1950
		Revised: 07/11/2024
		Next Review: 07/11/2026

Policy

The policy of the Department of Human Services (DHS) Office of Inspector General (OIG) Internal Investigations Unit (IIU) is that all information gathered during the course of an internal investigation will be maintained in a strict and confidential manner.

No one within the Office of Inspector General (OIG) will divulge any information obtained during an investigation to anyone who is not authorized to have that information, without prior approval from the Inspector General or his/her designee.

The following security measures will be taken with regard to internal investigation documents:

The Inspector General or his/her designee is the custodian of the internal investigation case files, which are to be maintained in locked cabinets at the State Office, or electronically stored in a secured access, controlled environment.

Reports, case files, and other relevant documents will be maintained in a secured environment while the investigation is active.

All exhibits will be properly marked / labeled with an exhibit number that corresponds to exhibit information listed in the final report.

Any physical evidence obtained by IIU staff will be logged onto a **Property / Evidence Control Record** and stored in a secured area within OIG. When no longer needed, the physical evidence will be returned to its owner or disposed of, whichever is applicable. This will be documented on the **Property / Evidence Control Record**, which will then be placed in the associated case file.

Any criminal history information obtained during an investigation must be destroyed upon completion of the investigation. **At no time is criminal history information to be stored within a completed case file.**

Authority

[O.C.G.A. § 49-2-1 et seq.](#)

[O.C.G.A. § 49-2-4 et seq.](#)

References

None

Applicability

This policy is applicable to all divisions and offices of DHS.

Definitions

None

Responsibility

1. The OIG Internal Investigations Unit Chief Investigator is responsible for oversight of POL 1950.
2. The OIG Internal Investigations Unit Chief Investigator develops, issues, and updates procedures to implement this policy.

History


Replaces POL 1950, last reviewed on 7/11/2024.

Evaluation

The OIG Chief Investigator evaluates this policy by:

1. Completing an annual internal review to confirm accuracy of the established guidelines.
2. Passing any review(s) with no findings.

1951 Authority and Responsibilities

	Department of Human Services Policy and Manual Management System	Index: POL 1951
		Revised: 07/11/2024
		Next Review: 07/11/2026

Policy

The policy of IIU is to investigate all complaints of alleged employee misconduct, including anonymous complaints, when possible, to determine the validity of the allegations and take appropriate action.

The OIG Internal Investigations Unit (IIU) is responsible for addressing allegations of misconduct by employees, contractors or others associated with the Department of Human Services (DHS). The goal of IIU is to: (1) identify such persons who engage in misconduct; (2) improve proficiency and efficiency through a review of policies and procedures identified during an investigation; and (3) protect employees against false allegations.

Authority and Responsibilities

The IIU has the authority and responsibility to engage in the following:

1. Initiate investigations as deemed necessary and appropriate the Inspector General or his/her designee.
2. Ensure that each investigation is handled in a professional, thorough, complete, timely and unbiased manner, using all approved techniques and resources made available to the investigative staff.
3. Refer matters that do not fall within the purview of the unit to the appropriate administrative and/or prosecutorial agencies, such as the Georgia Bureau of Investigation and/or the Office of the Attorney General.
4. Conduct joint investigations with other oversight or law enforcement agencies, or assist such agencies, as requested.
5. At the conclusion of the investigation, the assigned Senior Investigator will prepare a written report that contains the reported allegations, the findings of each allegation, a list of persons who were interviewed and a list of any evidence obtained during the investigation.
6. Engage in prevention activities, including but not limited to; training, education, and review of policies and procedures.
7. Maintain information regarding the cost of each investigation.

The IIU is provided the following powers to accomplish its responsibilities:

1. Open and conduct investigations as deemed appropriate the Inspector General or his/her

designee, as requested by agency or division leadership. With the approval of the IG, the Chief Investigator has the authority to make decisions regarding the method and scope of investigations, within the framework of established policies and procedures.

2. Require employees to cooperate and provide assistance, when appropriate, with any type of investigation regarding alleged criminal or administrative misconduct.
3. The right to obtain full and unrestricted access to all offices, employees, records, information, data, reports, plans, projects, contracts, memoranda, correspondence, and any other materials, including electronic data of employees that specifically relate to issues currently under investigation by the OIG.
4. Encourage employees to report to the OIG any information regarding abuse, neglect, exploitation, fraud, waste, corruption, or illegal acts.

Maintenance of Records and Files

The IIU maintains an electronic record of the allegations and outcomes of complaints against DHS employees on a case management database. Hard copies of the original reports and all associated evidence are secured in locked cabinets and maintained in accordance with all applicable state records retention schedules.

Confidentiality

The nature and source of internal allegations, the progress of the investigation, and the resulting materials are considered confidential information. The contents of the internal investigation files will be retained in a secured location within the area occupied and controlled by IIU OIG. The information and records of an internal investigation will only be released under the following circumstances:

Upon the approval by the Commissioner or his/her designee.

Upon the request of or at the direction of the Office of the Attorney General or a prosecuting entity.

Upon receipt of a court order.

At the request or direction of DHS' General Counsel, pursuant to an Open Records' request.

Authority

[O.C.G.A. § 49-2-1 et seq.](#)

[O.C.G.A. § 49-2-4 et seq.](#)

References

None

Applicability

This policy is applicable to all divisions and offices of DHS.

Definitions

None

Responsibility

1. The OIG Internal Investigations Unit Chief Investigator is responsible for oversight of POL 1951.
2. The OIG Internal Investigations Unit Chief Investigator develops, issues and updates procedures to implement this policy.

History


Replaces POL 1951, last reviewed on 7/11/2024.

Evaluation

The OIG Internal Investigations Unit Chief Investigator evaluates this policy by:

1. Completing an annual internal review to confirm accuracy of the established guidelines.
2. Passing any review(s) with no findings.

1952 Retention of Investigative Records

 <p>Department of Human Services Policy and Manual Management System</p>	Index: POL 1952
	Revised: 08/07/2023
	Next Review: 08/07/2025

Policy

The policy of the Department of Human Services (DHS) Office of Inspector General (OIG) Internal Investigations Unit (IIU) is the retention of case files to support the investigation from the original allegation to the final disposition.

Maintenance and Storage

Investigative files and related materials shall at all times be secured by the assigned investigator(s) while an investigation is ongoing. After an investigation has been finalized and closed, the case file, which would normally include a copy of the written report, supporting documentation, exhibits, and case notes, as well as any other relevant documents or items, should be kept in a locked, secure area that is restricted to authorized OIG personnel only.

Case files and associated documents for closed investigations should be retained in accordance with state retention requirements.

Once the retention requirements have been satisfied and case files are no longer needed, the destruction of those files shall be coordinated by the Chief Investigator and the Senior Investigator who was assigned to the case, if applicable. The method of destruction will be by shredding.

In some situations, the agency is requested or directed to preserve/save records, documents and other materials related to a matter that involved IIU staff. In those cases, IIU staff shall adhere to retention direction received from OGC staff regarding such matters.

Protection of Records during a Natural or Man-made Disaster

In the event of a natural or man-made disaster, the Chief Investigator and/or appointed designee will have the following responsibilities regarding the security of IIU's records: Ensure that copies of all ongoing and final investigative records maintained by the unit are secured and not in danger of being damaged or destroyed during civil unrest or natural disaster.

Ensure that all ongoing and investigative records remain secured on-site and/or are removed to another location where they can be secured until such time the records can be returned safely to the secured area within the OIG office.

Immediately notify the Inspector General (IG) and/or Deputy Inspector General of any potential threat to the safety and security of the investigative reports.

When possible, ensure that an authorized OIG staff member is stationed in the area to secure the records until further instructions are received from the IG or Deputy IG.

Authority

O.C.G.A. § 49-2-1 et seq.

O.C.G.A. § 49-2-4 et seq.

References

None

Applicability

This policy is applicable to all divisions and offices of DHS.

Definitions

None

Responsibilities

1. The OIG Internal Investigations Unit Chief Investigator is responsible for oversight of POL 1952.
2. The OIG Internal Investigations Unit Chief Investigator develops, issues, and updates procedures to implement this policy.

History


Replaces POL 1952, last reviewed 08/07/2023.

Evaluation

The OIG Internal Investigations Unit Chief Investigator evaluates this policy by:

1. Completing an annual internal review to confirm the accuracy of the established guidelines.
2. Passing any review(s) with no findings.

1953 Workplace Violence - External Threats

	Department of Human Services Policy and Manual Management System	Index: POL 1953
		Revised: 04/04/2023
		Next Review: 04/03/2025

Policy

The Department of Human Services (DHS) must protect its employees, contractors, and clients from harm while conducting official business on behalf of the Department or with the Department in a DHS Work Site. Therefore, the Department has created this policy to set forth the management of threats or acts of workplace violence by external sources, such as an employee spouse or acquaintance, a client(s), or contractor(s) providing services to the Department.

Scope

This policy shall apply when threats or acts of violence toward a DHS employee occur from an external source such as, but not limited to, a DHS customer, Employee of another agency, contractor, or the spouse or acquaintance of a DHS employee. The threat is made through verbal or written communication or the act of violence is carried out while conducting official business with DHS at a DHS worksite.

NOTE This policy is separate and distinct from DHS Office of Human Resources Policy 110 and all attachments.

Definitions

Assault

To attack someone physically or verbally, causing bodily or emotional injury, pain, and/or distress. This might involve the use of a weapon, and includes actions such as hitting, punching, pushing, poking, or kicking.

Dangerous Weapon

A device, instrument, or substance that is used for, or is readily capable of, causing death or serious bodily injury. These include guns, knives, clubs, chemicals, and explosive devices.

Department of Human Services (DHS) Work Site

A building, residence, facility, or part thereof, where its employees or contractors are present to perform their official duties.

Domestic Violence

A reference to acts of physical and psychological violence, including harassing or intimidating behavior that occurs as part of personal relationships. Included in the concept of domestic violence are spousal abuse, abuse among intimates, as well as sexual and physical abuse of children, the elderly, or the infirm.

Employee Assistance Program (EAP)

A professional assessment, referral, and short-term counseling service is available to all DHS employees and, in some situations, to their family members to help with personal problems such as substance abuse, financial pressures, job stress, and family dysfunction which may be affecting work performance. EAP services are voluntary, confidential, and provided at no cost to the employee.

Intimidating or Harassing Behavior

Threats or other conduct that in any way creates a hostile environment, impairs agency operations; or frightens, alarms, or inhibits others. Psychological intimidation or harassment includes making statements that are false, malicious, disparaging, derogatory, rude, disrespectful, abusive, obnoxious, insubordinate, or which have the intent to hurt others' reputations. Physical intimidation or harassment may include holding, impeding, or blocking movement, following, stalking, touching, or any other inappropriate physical contact or advances.

Local Authorities

Municipal, county, state, and federal law enforcement (having local responsibilities); or public safety personnel, such as police, firefighters, arson investigators, bomb/threat investigators, etc., of the civil jurisdictions where Department facilities are located or acts of violence occur.

Sabotage

An act to destroy, damage, incapacitate, or contaminate property, equipment, supplies, or data (e.g., hard copy files and records, computerized information, etc.); to cause injury, illness, or death to humans; or to interfere with, disrupt, cripple, disable, or hinder the normal operations or missions of the Department of Human Services.

Stalking

A malicious course of conduct that includes approaching or pursuing another person with the intent to place that person in reasonable fear of serious bodily injury or death to him/herself or a third party.

Threat

Any oral or written expression or gesture that could be interpreted by a reasonable person as conveying an intent to cause physical harm to persons or property. Statements such as, "I'll get him", "She won't get away with this" or "That's why people blow things up" could be examples of threatening expressions depending on the facts and circumstances involved.

Workplace Violence

An action (verbal, written, or physical aggression) which is intended to control or cause, or can cause, death or serious bodily injury to oneself or others, or property damage. Workplace violence includes abusive behavior toward authority, intimidating or harassing behavior, and threats.

References

O.C.G.A. § 50-18-72(25)

General Provisions

1. Employees, Clients, and Vendors have a right to expect to conduct business either with or on behalf of the Department in a safe, professional, and business-like manner.
2. DHS will not tolerate any threats or acts of violence being carried out by any person conducting business with the department or any other interactions with department personnel during the course of their work assignments, this includes but is not limited to customers, vendors, or associates (spouse, friend, significant other, etc.) of anyone who is employed by the Department.
3. Examples of prohibited behavior that shall be reported include but are not limited to:
 - a. Threatening, abusive, or intimidating language or written material.
 - b. Fighting or acts of violence directed toward the Department's employees.
 - c. Stalking.
 - d. Possession of weapons on DHS property unless specifically authorized.
4. All employees should remain alert and be familiar with their surroundings to recognize potentially serious situations. Most acts of workplace violence are preceded by direct and/or indirect threats. Employees at all levels must, therefore, take all threats seriously and report them as soon as possible.

Warning Signs

1. Individuals may exhibit certain behaviors that may be warning signs of potentially violent behavior, whether in person or on the phone. Below are some examples of warning signs:

Visual cues when in person

- a. Easily frustrated or angered.
- b. Scowling and sneering.
- c. Pacing, restless, or repetitive movements.
- d. Clinched jaw or fists.
- e. Glaring or avoiding eye contact.
- f. Violating personal space.

Verbal cues when in person or on the phone

- a. Swearing or emotional language.
- b. Change in voice or tone.
- c. Refusing to follow directions or to comply with procedures.
- d. Threatening statements directed toward staff or work sites.

Establishing a Plan

1. Divisions should ensure that their assigned offices are responsible for establishing a written plan to prevent workplace violence and manage incidents and/or threats in each location. The plans will be subject to a review by OIG during investigations or other times a review is warranted. Some examples of what must be considered in the plan are as follows:
 - a. Establish facility entrance requirements such as signing in and wearing badges when appropriate.
 - b. Ensuring areas are secured where cash is accepted or handled.
 - c. What to do in the case of a threat or act of violence against the facility or employees.
 - d. List of local law enforcement numbers (911, Non-Emergency Numbers, etc.)
 - e. Evacuation routes or safe zones within the facility.
 - f. Training for all staff that works in the location.
 - g. Designation of who has authority to make emergency decisions regarding office closure or emergency dismissal from the worksite.
 - h. Process for obtaining restraining orders for individuals that department believes this action is necessary to protect staff at a DHS worksite.

NOTE

A restraining order may be sought by the Department on behalf of employees under circumstances where employees are threatened or harmed due to the performance of work-related duties.

- i. Designation of long-term return to work plan as needed. The division or office may stipulate that they will follow the procedures as outlined in their Continuation of Operations Plan (COOP).
2. Division/Offices will designate a person (Director, Manager, or Supervisor) and a secondary backup who will be the central point of contact for providing information to their respective areas/offices on the handling of incidents/threats. Examples would be helping to determine the need (if not already decided) to contact law enforcement, a decision to prohibit someone from coming back to the location or other offices, etc.

Reporting of Acts or Threatened Acts of Violence (External Source)

1. Employees are responsible for notifying their Supervisors or other authorized officials of all acts or threats of violence. Employees will be expected to follow the workplace violence reporting plan established in their Division/Office location regarding reporting of such acts or threatened acts of violence.
2. Any recurring or continuing acts or threatened acts of violence on or off the work premises should be immediately reported in compliance with your Division/Office's workplace violence reporting plan.

3. All acts or threatened acts of violence are to be taken seriously, including anonymous reports.
4. Employees failing to make such reports will be subject to disciplinary action as stated in DHS Office of Human Resources Policy 110.
5. A Workplace Violence or Threats of Violence-External report (see attachment #1) must be completed within three (3) business days after the incident and submitted to the DHS Office of Inspector General (OIG) for review and filing. OIG will respond that the report has been received and is under review.
6. OIG will respond in writing to the reporting person, that no follow-up is needed or that OIG will open an investigation into the incident.
 - a. If employee misconduct is involved, OIG will notify the Office of Human Resources (OHR) as to the employee's reported actions. Unless there is a criminal element, OHR will investigate the employee's actions and follow its normal procedures to determine if the actions of the involved employee(s) violated any DHS policy and what further action is warranted.
 - b. If there is no employee misconduct then the report will be filed for history, tracking, and information purposes. It is expected that the local law enforcement agency will handle any criminal charges that arise from the incident.

Handling of External Customers

1. It is expected that each division or office will follow their current protocols for the management of customers that have been barred from in-person visits to an office or worksite.
2. OIG will not make recommendations or decisions on how customers are to be managed after an incident has occurred.

Staff Training Requirements

The following are the training requirements for this policy.

1. A list of Frequently Asked Questions (FAQs) will be posted on the DHS website. These FAQs will provide general answers to questions about Workplace Violence (External Threats) and the reporting process.
2. Training for all employees will be provided through the Learning Management System utilizing the current Workplace Violence Module(s). That module will include general guidelines on how to detect, respond, and report workplace violence threats from an external source.
3. In addition to the general training for all employees, each office must conduct semi-annual training for all employees for procedures outlined in their local workplace violence safety plan and include the same training in any local orientation for new hires. This training shall be documented with the outline of the training, who provided the training, the date of the training, and a sign-in sheet for all attendees. This documentation is subject to review by the Office of Inspector General for investigative purposes or as requested.

History

None

Evaluation

The Office of Inspector General will evaluate this policy in the below manner:

- Evaluation of incident rates over time.
- Accuracy of offices following procedures outlined in safety plans.
- Random reviews of training documents in DHS offices.