

Template Whistleblower Case Management Proceduresⁱ

Purpose: The purpose of this document is to formalize safe, effective, and consistent whistleblower case management procedures as the **[MEMBER OFFICE OR COMMITTEE]** (hereinafter, “Office”) engages with whistleblowers from the public and private sectors in support of the Office’s oversight work **[AND CONSTITUENT SUPPORT FUNCTIONS]**. This document provides key practices for internal Office procedures and for external communications with a potential whistleblower (hereinafter “whistleblower”).

Decision Makers(s): The **[MEMBER/CHAIR/RANKING MEMBER]** has responsibility for making the key decisions affecting the Office’s collection, retention, and use of all information related to whistleblower matters.

Manager: The manager for overseeing and implementing these procedures is the Office’s **[INSERT TITLE]**.

Office Training Requirements: Staff authorized to work with whistleblowers must complete the training Best Practices for Working with Whistleblowers and review the accompanying manual. The manager must be certified in the Working with Whistleblowers Curriculum and may also designate other staff to become certified.ⁱⁱ

Additional Guiding Resources: The Office of the Whistleblower Ombuds has developed resources for working with whistleblowers, including the templates referenced throughout this document, available at <https://whistleblower.house.gov/resources/guidance-documents>. The Office of the Whistleblower Ombuds also provides confidential case consultations to guide staff in their work with whistleblowers.

Intake

Internal Office Procedures

1. The Office’s available method(s) for receiving whistleblower disclosures include:
 - **[INSERT, e.g., web-based form,ⁱⁱⁱ hotline, designated email, in-person]**
2. Designated staff
 - Staff authorized to work with whistleblowers must complete the training, Best Practices for Working with Whistleblowers and review the accompanying manual.^{iv}
 - Front office staff should also be familiar with how to identify potential whistleblower matters and communicate them to the Office’s manager.

ⁱ This document was informed by best practice guidance developed by the Office of the Whistleblower Ombuds, an independent and nonpartisan House support office.

ⁱⁱ The Office of the Whistleblower Ombuds provides a live and on-demand version of its foundational training, Best Practices for Working with Whistleblowers, as well as a Working with Whistleblowers Curriculum. Additional information is available at <https://whistleblower.house.gov/trainings>.

ⁱⁱⁱ The Office of the Whistleblower Ombuds has developed a Template Intake Webform. A preview is available at <https://whistleblower.house.gov/sampleintakeform>, and all downloadable templates are available at <https://houseset.house.gov/campus/service-providers/office-of-the-whistleblower-ombuds/documents>.

^{iv} The Office of the Whistleblower Ombuds provides a live and on-demand version of its foundational training, Best Practices for Working with Whistleblowers, as well as a Working with Whistleblowers Curriculum. Additional information is available at <https://whistleblower.house.gov/trainings>.

3. The Office will use the following procedures to keep whistleblower-communications secure (see Template Whistleblower Confidentiality Policy for full list of procedures).
 - Document whistleblower intake in the Office's secure tracking system.^v
 - Ensure personally identifiable information (PII) is handled appropriately.^{vi}
 - Ensure sensitive or classified information is handled lawfully.^{vii}
 - After initial intake, create a separate case file for each whistleblower with key information that can be updated as needed to reflect the case status, referrals, follow-up, and other notes and files (see Template Whistleblower Tracking Sheet).
 - Limit access to designated staff, and on a need-to-know basis.

External Communication with the Whistleblower

1. Before the Office gathers information from the whistleblower, share key disclaimers electronically (e.g., via webform or email) or during the Office's initial communications (see Guiding Phrases for Working with Whistleblowers).
 - Acknowledge that whistleblower protections exist for communicating with Congress, but the Office cannot provide legal advice.
 - (As applicable) Acknowledge the potential for retaliation and advise the whistleblower to consult experienced counsel for legal guidance (see Whistleblower Support Organizations and Legal Resources^{viii}).
 - Caution the whistleblower against communicating with the Office through their work resources.
 - Provide an overview of the Office's jurisdiction **[INSERT JURISDICTION]**.
 - Advise the whistleblower not to submit classified information or other information barred from release through unsecure channels. If the disclosure may involve classified materials, pause and consult the Office of the Whistleblower Ombuds and the House Security Office for guidance.
 - Inform the whistleblower of their right to confidentiality under the House Code of Conduct.
2. Explain the Office's processes, to provide transparency and manage expectations.
 - Be transparent about any limitations (e.g., jurisdiction, bandwidth).
 - Convey the Office's commitment to provide assistance when possible, and preview that you will provide guiding resources to support the whistleblower's process.
 - Let the whistleblower know they should expect to hear back within **[INSERT REALISTIC TIMEFRAME]**.

v The House has developed standards for the electronic and physical protection of sensitive information. These standards can be applied to your office's development of a secure tracking mechanism for whistleblower communications, "HISPOL 010.0, Protection of Sensitive Information," available at <https://housenet.house.gov/technology/policies-and-standards>. House Information Resources can assist your office in developing a separate secure OneDrive that can only be accessed by designated individuals.

vi Personally Identifiable Information (PII) includes any information that can be used to determine an individual's identity, including name, date of birth, Social Security number, or other types of information that can be traced to an individual, such as employment, medical, financial, and educational information. The House Office of the Sergeant at Arms provides additional guidance for the handling of PII, available at <http://saa.house.gov/ohs/personally-identifiable-information-pii.shtml>.

vii Classified conversations should be coordinated with the Office of House Security, available at <https://sgtatarms.house.gov/ohs/>. Further, the House has developed standards for the electronic and physical protection of sensitive information, "HISPOL 010.0, Protection of Sensitive Information," available at <https://housenet.house.gov/technology/policies-and-standards>.

viii The Office of the Whistleblower Ombuds has developed a menu of nongovernmental whistleblower support organizations and legal resources, available at <https://whistleblower.house.gov/whistleblower-support-organizations>.

3. Gather key facts for pre-screening, potential follow-up, and to inform prioritization step.
 - Ask guiding questions to obtain key facts (for full list of questions, see Model Intake Form).
 - ◆ (Non-work) contact information?
 - ◆ Employment status and employer?
 - ◆ Summary of disclosures?
 - ◆ Have disclosures been made elsewhere?
 - ◆ Goals in working with the Office?
 - To mitigate risk for the whistleblower and the Office, refrain from accepting documentary evidence at this stage.
4. Establish ground rules with the whistleblower (see Template Whistleblower Confidentiality Policy for a full list of ground rules).
 - Discuss whether the whistleblower wants to be a confidential or public source.
 - Share the Office's confidentiality policy, which includes a reminder around limitations.
 - Discuss whether the whistleblower wants to place boundaries around the use of the information they shared.

Prioritization

Internal Office Procedures

1. Office briefing
 - As appropriate, brief the manager on the whistleblower's key facts.
 - In consultation with the manager, use the key facts to determine whether additional staff need to be involved; how the Office will prioritize the matter; and which guiding resources to share with the whistleblower.
2. The Office uses the following guidelines to help determine if it will look into a matter further:
 - Is it a whistleblowing matter, or was the reprisal action triggered by whistleblowing?
 - Is it a matter within the Office's **[INSERT JURISDICTION AND PRIORITIES]**?
 - Is it an urgent issue, such as a national security threat or danger to public health?
 - Does it concern systemic breakdowns within the public or private sectors?
 - Is the whistleblower a constituent?
3. Document the prioritization determination within the Office's secure tracking system.

External Communication with the Whistleblower

1. Clearly communicate with the whistleblower regarding how the Office will be proceeding, moving forward. Where applicable, reiterate the types of disclosures the Office will pursue, and explain how the Office cannot pursue all disclosures.
2. Discuss updated timelines for follow-up, as applicable.

3. Where the Office will not be pursuing the disclosure, still share guiding resources in an effort to conclude on good terms and provide the whistleblower a menu of applicable referral options where appropriate (see Office of the Whistleblower Ombuds' Whistleblower Audience page^{ix}).

Referral

Internal Office Procedures

1. Review the Office's Referral Tip Sheet for easily accessible information on the different governmental and nongovernmental options for whistleblowers to report allegations of misconduct and retaliation (see Referral Tip-Sheet).
2. Document the various referral options shared with the whistleblower within the Office's secure tracking system, as well as any actions the Office is taking for direct referrals.

External Communication with the Whistleblower

1. Consider additional questions at this stage to inform the referral process, including any developments since the initial intake (e.g., have their goals changed, have they experienced subsequent retaliation, have they contacted other House or external offices?).
2. Share a menu of relevant referral options with the whistleblower, including actions the Office is considering, and discuss potential risks and benefits.
3. Obtain the whistleblower's consent before making a referral on their behalf.

Follow-Up (Working with the Whistleblower Moving Forward)

Internal Office Procedures

1. Identify the staff contact for each case to ensure a clear point of contact for the whistleblower and to be the lead on related follow-up actions.
2. Identify realistic target timeframes for completing follow-up actions.
3. Refer to the Office's checklist of potential follow-up actions (see Follow-Up Checklist).
4. Document actions taken within the Office's secure tracking mechanism.

External Communication with the Whistleblower

1. Communicate when the whistleblower should expect to hear updates and ensure the communication occurs, even if the Office chooses not to act on the disclosure.
2. Check in with the whistleblower as appropriate to share respective developments, actions taken, and responses.
 - Have they made their disclosure elsewhere?
 - Was the issue resolved by their employer?
 - Have they experienced delayed retaliation?

ix The Office of the Whistleblower Ombuds has developed a Whistleblower Audience page that includes a menu of governmental and nongovernmental public-facing resources, available at <https://whistleblower.house.gov/whistleblower-audience>.

3. Ask for the whistleblower's expertise as appropriate to support the Office's related oversight.
 - Can the whistleblower suggest document requests the Office might make?
 - Would it be helpful for them to clarify obscure concepts and identify correct terminology?
 - Are they able to matchmake the Office with additional witnesses?
 - Can they help the Office brainstorm around policy solutions and hearing questions?
4. Discuss additional actions to support the whistleblower and advance the Office's oversight work where appropriate (see Follow-Up Checklist for a full list). For instance, the Office may:
 - Open or request an investigation into the alleged wrongdoing.
 - Inquire on the status/request a briefing of an investigation by the relevant government whistleblower office (see Template Privacy Act and HIPAA Release for a sample Privacy Act release, when necessary).
 - Send a "warning letter" (see Sample Letter to Employer) that it is illegal to retaliate against a congressional witness.^x
 - Explore legislative solutions to address systemic threats exposed by the disclosures.
5. Incorporate ground rules before acting on the whistleblower's information.
 - Request permission before sharing the disclosure – or related information that could identify the whistleblower – outside of your office (see Template Consent to Publicly Disclose Whistleblower's Identity).
 - Provide the whistleblower the opportunity to discuss and/or review potential communications around their information so that they can ensure it is accurate and maintains their confidentiality to the extent desired.

^x A warning letter is a useful tool to help deter retaliation against a congressional witness. However, it is important to weigh the specific circumstances involved in each case and manage expectations around your office's involvement. For instance, a congressional office may be willing to send a support letter but not willing to serve as a witness in subsequent litigation. Conversely, an office may not place limitations around support for their witnesses. Consult your office's counsel before making any commitments that you may not be able to honor. For further guidance, see "Holding Retaliators Accountable," available at https://whistleblower.house.gov/sites/whistleblower.house.gov/files/Holding_Retaliators_Accountable.pdf.