OFFICE OF THE
WHISTLEBLOWER OMBUDS

MAINTAINING WHISTLEBLOWER CONFIDENTIALITY

OVERVIEW

The Code of Official Conduct for the House, as amended in the 117th Congress, mandates the protection of whistleblower confidentiality.[i] The Office of the Whistleblower Ombuds stands ready to assist you with compliance, training, and consultation concerning these confidentiality requirements. The measures provided in this guidance document are intended to protect the whistleblower's information, as well as the security of Congress' investigative and oversight work. This document was developed in consultation with the Office of Cybersecurity and the Office of House Security.

WRITTEN PROCEDURES

Written procedures for handling whistleblower information and communications with whistleblowers are essential for establishing and maintaining effective and safe relationships with whistleblowers, including protecting their confidentiality when applicable. Consider incorporating your office's existing procedures for handling sensitive information into your procedures for working with whistleblowers and addressing the elements below.[ii,iii]

- Identify **who** in the office will make key decisions concerning the subsequent use of any whistleblower information.
- Describe **why** the information is being collected and what its likely subsequent uses are.
- Plan for an early discussion with the whistleblower concerning the **level of confidentiality** they desire while:
    - Counseling the whistleblower that this decision should be made through talks with their attorney and loved ones;
    - Managing expectations by alerting the whistleblower to the office's **inability to guarantee confidentiality** (because of enhanced external surveillance techniques and limited confidentiality legal requirements, for example), while still committing to taking all actions within the office's ability to maintain the whistleblower's confidentiality and comply with the Code of Official Conduct.
- Identify **what** information is to be collected and what portion of that information will be considered sensitive. A case-by-case decision concerning confidentiality will inform this evaluation.
- Describe the **notice and consent** procedures afforded to the whistleblower concerning the collection, use, and sharing of the information.
- Discuss the procedures, protocols, and controls that will be utilized to ensure the **confidentiality** of the information, including:
    - Restricting access to the information to those with a strict need to know;
    - Encrypting electronic information (especially on portable devices such as laptops, thumb-drives, and CDs);
    - Labeling removable media such as external disks and thumb-drives;
    - Labeling and securely storing hard copies of sensitive whistleblower information; and
    - Procedures for **communicating** safely with the whistleblower and potential third parties:
        - Use encrypted channels for communicating sensitive information;[iv]
        - Label, securely wrap, and affirmatively track hard copies and removable electronic media when in transit; and

        - When requested, protect the confidentiality of the whistleblower. Consider:
            - In-person meetings or the Postal Service; and
            - Higher assurance anonymizing communication tools.[v]
- Identify potential third-parties with whom the information might be **shared** – e.g., other Congressional entities, congressional liaisons, and Inspectors General. Incorporate into these procedures:
    - On a case-by-case basis, rules or guidelines for use and for further sharing by third parties; and
    - Awareness of the need for stripping or masking **identifying information** from any information shared (remember: often a whistleblower's information is highly specific in nature or known to such a small circle that their "facts are their signature") and any **metadata** – e.g., track changes and phone location – when whistleblower confidentiality is requested.

GROUND RULES

In addition, these procedures may include some foundational **ground rules** for working with whistleblowers, such as:

- Communicate through a whistleblower's attorney whenever possible instead of directly with the whistleblower, to invoke the client-attorney privilege;
- Identify alternative channels to obtain a whistleblower's evidence – e.g., direct requests to the employer for documentation – while being careful not to provide a level of specificity that could be traced back to the whistleblower, and consider working through a nonprofit organization or other trusted entity that can serve as a buffer and reduce paper trails; and
- A **vital survival tip**: Encourage the whistleblower to engage in whistleblowing on their own time, with their own resources, using secure communication platforms.

CYBER BEST PRACTICES

To further ensure the **confidentiality** of sensitive whistleblower information, the office should establish adequate cybersecurity protocols for systems storing or processing that information and the network environment where those systems reside.[vi] As a suggested minimum, these systems should:

- Maintain adequate cyber best practices. Work with the Office of Cybersecurity to ensure that systems are configured in line with House standards and are routinely patched.

STAFF TRAINING

The office should ensure adequate staff **awareness** and training concerning the handling and protection of whistleblower information.

- Consider having staff take "Best Practices for Working with Whistleblowers," the Office's weekly webinar hosted by the Congressional Staff Academy, https://whistleblower.house.gov/events/virtual-training-best-practices-working-whistleblowers.

ADDITIONAL RESOURCES

- House Office of the Whistleblower Ombuds, https://whistleblower.house.gov/, x66638, WhistleblowerOffice@mail.house.gov.

- House Office of Cybersecurity, https://housenet.house.gov/campus/service-providers/cybersecurity, cybersecurity@mail.house.gov.
- Office of House Security, http://sgtatarms.house.gov/ohs/ (for questions concerning handling of classified information).
- A list of Whistleblower Support Organizations, https://whistleblower.house.gov/whistleblower-support-organizations.

Please Note: The House Office of the Whistleblower Ombuds DOES NOT receive whistleblower disclosures. It is an independent nonpartisan support office established to advise House offices on best practices for working with whistleblowers.

---

[i] Clause 21 of Rule XXIII, House Code of Official Conduct reads (emphasis added):

> (a) Except as provided in paragraphs (b) and (c), a Member, Delegate, Resident Commissioner, officer, or employee of the House shall not knowingly and willfully disclose publicly the identity of, or personally identifiable information about, any individual who has reported allegations of possible wrongdoing, including retaliation, under processes and protections provided by the Civil Service Reform Act of 1978, the Whistleblower Protection Act of 1989, the Intelligence Community Whistleblower Protection Act of 1998, or any other Federal law that establishes the right for individuals to make protected disclosures to Congress.
>
> (b) The limitation in paragraph (a) shall not apply to any disclosure of an individual's identity or personally identifiable information if—
>
> (1) the individual has provided express **written** consent prior to such disclosure;
>
> (2) the individual has already voluntarily and publicly disclosed their identity; or
>
> (3) the disclosure is by the chair of a committee after an affirmative vote by two-thirds of the members of the committee that such disclosure is in the public interest.
>
> (c) Nothing in this clause shall prevent—
>
> (1) an investigation of any allegation of wrongdoing disclosed by any individual; or
>
> (2) the public disclosure of substantive information shared by any individual that is not personally identifiable to that individual.
>
> (d) Disclosures made pursuant to paragraph (b)(3) shall be subject to appropriate safeguards, including that the individual be provided timely advance notice if possible before their identity or any personally identifiable information is disclosed prior to the vote described in paragraph (b)(3), unless such information would jeopardize the related investigations. When providing such notice to the individual the committee chair shall send the individual a **written** explanation of the reasons for the disclosure.

[ii] This guidance has been adapted from the Privacy Impact Assessment format found in Section 208 of the E-Government Act of 2002, P.L. 107-347, 116 Stat. 2899 (Dec. 17, 2002), *available at* https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf, Office of Management and Budget Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," (Sept. 26, 2003) *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf, and the Federal Trade Commission's Fair Information Practice Principles reported on in "Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress", Federal Trade Commission (May 2000), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[iii] The handling of classified information, including classified conversations, should be coordinated with the Office of House Security, *see* http://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/sites/housenet.house.gov/files/documents/hispol_010_0_-_information_security_policy_for_the_protection_of_sensitive_information.pdf.

[iv] Consult the House Office of Cybersecurity when contemplating tools for encrypted communications.

[v] These tools will demand substantial resources and technical sophistication to be effective; consult the House Office of Cybersecurity.

[vi] *See* "House Information Security Policy for the Information Security Compliance Program," HISPOL 007.0, *available at* https://housenet.house.gov/sites/housenet.house.gov/files/documents/hispol_007_0_-_information_security_policy_for_the_information_security_compliance_program.pdf.