OFFICE OF THE
WHISTLEBLOWER OMBUDS

INFORMATION SECURITY

OVERVIEW

Hand in hand with the issue of protecting a whistleblower's confidentiality are the technical and administrative controls you develop and implement to provide effective security for the whistleblower's information.

The House already operates within a secure environment, and it is exploring additional measures to enhance information security, but it is impossible to eliminate all risk. Ever-changing technology compounds the challenges of risk mitigation; however, it can also provide advanced tools to protect whistleblowers and their information. The Office of Cybersecurity can help vet encryption tools and other security software.

In addition to software tools, there are administrative and technical safeguards that your office can put in place to help protect whistleblower information and communications. These practices should be formalized and used in conjunction with the ground rules you establish around the use of the whistleblower's information.

This fact sheet will provide guidance for analyzing your information security requirements for working with whistleblowers and for the development of a secure tracking system.

PROTOCOLS TO KEEP WHISTLEBLOWER INFORMATION SECURE

Protecting a whistleblower's information often goes beyond simply protecting their name and address. A whistleblower's information is highly specific in nature or known to such a small circle that their "facts are their signature." Clause 21 of the House Code of Official Conduct, which protects whistleblowers' confidentiality, captures this concept by extending protection to the "**personally identifiable information**" of a whistleblower.

This serves as a reminder that a whistleblower's facts can be considered sensitive information.
In addition to the Code of Official Conduct, House information security policy stipulates that information that *relates* to an identifiable individual who provided information to your office in confidence, or with restrictions on its use, is considered sensitive information and requires a heightened degree of protection. This, of course, includes information such as the name, address, and phone number of a whistleblower, but in some cases this will include some or all of the facts of the case, as well. The degree of confidentiality the whistleblower requests will also inform the analysis of what is sensitive information.

Impact Assessment

Development of a written protocol to keep whistleblower information secure begins with an **impact assessment**. This can be thought of as an analysis of how that sensitive information is collected, stored, shared, and managed. This analysis and any other information security processes relevant for protecting whistleblower information should leverage your office's and the House's existing information security systems and procedures – build from existing frameworks rather than recreate them from scratch. This includes any existing office policies for the handling of classified or other sensitive information.

The impact assessment will be the foundation for identifying your requirements for protecting a whistleblower's information and their confidentiality, when applicable. Consider developing a generalized impact assessment that can be tailored for particular whistleblower cases as they arise. Working with whistleblowers and their sensitive

information can be a complicated and dynamic process – having a written template can structure your office's response to the complexities of the case and engender a nimble response.

The following considerations are useful when developing either a generalized or a case-specific impact assessment.

1) **Identify who in your office will make key decisions concerning:**
    a) The reason and purpose for the collection of the information;
    b) The implementation or execution of this impact assessment; and
    c) The subsequent use of the information.
2) **Describe why the information is being collected** – for example, to further the office's oversight goals.
3) **Identify the intended use of the information** – for example, to assess the validity and extent of the alleged misconduct, to guide investigations and oversight of the alleged misconduct, and to inform legislation to address the alleged misconduct.
4) **Incorporate a plan for an early discussion concerning the level of confidentiality the whistleblower is requesting.**
5) **Identify what information is to be collected and what portion of that information will be considered sensitive whistleblower information.** For example, consider the following categories of whistleblower information.
    a) Personally-identifiable information, such as:
        (1) Name, age, address, title, work history, salary, and any medical conditions; and
        (2) Employer, location, department, division, section, supervisors, and projects.
    b) Fact and narrative-specific information:
        (1) Substance of the disclosure (Remember: their facts may be their "signature");
        (2) Timelines of alleged misconduct, disclosures, and retaliation;
        (3) Privacy Act, HIPAA, trade secrets, or similar information;
        (4) Documentary evidence – for example, emails, notes of conversations, and photos; and
        (5) Metadata associated with documentary evidence – for example, track changes and phone location data.
    c) Classified or other sensitive information – consult the Office of House Security for specific guidance concerning the lawful handling of classified information.
6) **Describe the notice and consent procedures afforded to the whistleblower concerning the collection, use, and sharing of their information.** For example, see the list of whistleblower's rights on page 5, below.
7) **Identify the procedures, protocols, and controls that will be utilized to ensure the confidentiality of the information.** Consider addressing the following elements:
    a) Restrict access to the information to those with a need to know;
    b) Protect the sensitive information while it is **stored or processed**, whether it is stored electronically or on paper. This includes encrypting sensitive electronic information, certainly on portable devices and

including removable media such as external disks, thumb-drives, and CDs,[1] but it also includes secure physical storage, proper labelling, implementation of cybersecurity best practices, and staff training. See the Secure Tracking System section below for further guidance;

c) Protect the sensitive information while in **transit**, whether that is via electronic communication or the Postal Service and including removable media sent via the Postal Service or handed over in person. These protections apply for communications with the whistleblower as well as communications with third parties. See the Secure Tracking System section below for further guidance; and

8) **Identify with whom the information might be shared** – for example, other Congressional entities, congressional liaisons, and Inspectors General. (Guidance for protecting the information *when* it is shared is discussed below.) Keep in mind to:

a) Incorporate relevant legal, regulatory, and policy requirements, including clause 21 of the Code of Official Conduct, that concern protection of whistleblower confidentiality; and

b) Consider guidelines for evaluating the eventual publication of some of the whistleblower's information.

9) **Describe additional protocols to use when sharing whistleblower information with third parties is contemplated.** Remember to:

a) Identify rules and guidelines for use and for **further sharing** by third parties;

b) Incorporate procedures for stripping or masking **identifying information** ("facts are a whistleblower's signature"), and any metadata – for example, track changes and phone location data – when whistleblower confidentiality is requested;

c) Utilize appropriate communications channels when sharing or exchanging whistleblower information with third parties (see above and the Secure Tracking System section below for further guidance); and

d) Consider the possibility that the whistleblower will not consent to further sharing or that the information cannot be safely shared outside the immediate office.

10) **Identify relevant actions during the life cycle of the sensitive whistleblower information** – especially concerning the potential publication of the information, its retention and destruction.

11) **A case-specific impact assessment warrants a periodic review as the case develops.** The whistleblower may want to tighten or loosen the restrictions around the use of their information as circumstances change, and especially in cases where the whistleblower wishes to maintain confidentiality. Consider reviewing the impact assessment when:

a) The scope of the oversight or investigation expands and other entities – for example, agencies and additional whistleblowers – become involved;

b) Media involvement is warranted or considered, or occurs without the office's prior knowledge; and

c) When converting paper-based records to electronic systems or converting from one electronic system to another.

12) **The office's generalized impact assessment concerning whistleblower information should be periodically reevaluated and updated as necessary to ensure it remains relevant, clear, and actionable.** Also, consider

[1] Effective March 31, 2021, the House Chief Administrative Officer has disabled access for USB storage devices on all House desktop and laptop computers.

making your office's generalized impact assessment concerning whistleblower information publicly available.[2] Maintaining transparency concerning the impact assessment and your office's goal of protecting whistleblower information may lead to more effective relationships with whistleblowers and it may help ensure that your office's best practices remain fresh and valuable.

SECURE TRACKING SYSTEM

With a solid conceptual framework for handling whistleblower information established, consider the technical, administrative, and personnel measures that will help your office successfully implement that framework. The secure tracking system you use may be a paper-based system, a segregated server environment, or part of the office's existing IT infrastructure. The communication system you use may be the Postal Service or encrypted email. The implementation may vary depending on the circumstances of a particular whistleblower case, and it may change during the course of working with a whistleblower. Regardless, with your impact assessment in hand you can now identify the information security **functional requirements** that will help your office meet its goal of ensuring confidentiality for the whistleblower information.

As you develop or refine your secure tracking system and identify and implement the communications methods you will utilize, consider the following elements:

1) RESTRICT ACCESS TO INFORMATION.

a) Identify those with a need to know and regularly review this list.

b) Ensure adequate access controls are in place to enforce the need to know and regularly monitor the scope of access.

2) STORE INFORMATION SECURELY.

a) Paper or hard copies are:

(1) Retained in a locked room, cabinet, or drawer; and

(2) Labeled.

b) For electronically stored information, be sure to:

(1) Encrypt sensitive information at rest on portable devices – for example laptops, phones, and including off-line storage such as thumb-drives, CDs, and external disks.[3] Consider encrypting all sensitive data at rest, including data residing on desktops;

(2) Label removable media appropriately; and

(3) Use official House systems only - no personal devices, including removable media, for example.

3) COMMUNICATE INFORMATION SECURELY.

a) When exchanging information with the whistleblower and when sharing whistleblower information with third parties, ensure that whistleblowers' sensitive information is:

(1) Encrypted, when communicated electronically. Remember to:

[2] Public release would not be indicated if its publication would raise security concerns or reveal classified or sensitive information. In such instances, the impact assessment should be protected and handled in ways consistent with the Freedom of Information Act.

[3] See footnote 1.

i) Provide encrypted electronic communications channels;[4]

ii) Strive to have whistleblowers use the secure channels when communicating sensitive information with your office.

(2) Labeled, securely wrapped, and affirmatively tracked when hard copies or removable media are in transit.

i) Electronic storage devices and removable media should be encrypted and labeled as well.

b) When the whistleblower has requested, or circumstances warrant, heightened confidentiality protection, consider technical and non-technical means of supporting that requirement, such as:

(1) In-person meetings or the Postal Service (again while remembering to label hard copies, and label and encrypt removable media); and

(2) Sophisticated, open-source or commercial anonymizing electronic communication tools,[5] understanding that these tools may demand substantial resources and technical sophistication to be effective.

4) MAINTAIN CYBERSECURITY BEST PRACTICES.

a) If your office is storing, processing, and transmitting whistleblower information on electronic systems, your office's ability to support the confidentiality of that information will depend, in part, on the cybersecurity posture of those systems and connected networks. Consult with your office's technology partner and the Office of Cybersecurity to consider current **cybersecurity best practices** for those systems storing or processing sensitive whistleblower information and the network environment where those systems reside:

(1) Ensure that these systems are in compliance with House standards, patched, and up to date with current cybersecurity guidance.

(2) Ensure that your data has adequate protection. Specifically, maintain inventories of sensitive information and establish secure, regular automated backups and redundancies of key systems.

5) HAVE OFFICE STAFF WELL-TRAINED ON INFORMATION SECURITY PROCEDURES.

a) The best cybersecurity defense in an office is its knowledgeable and motivated staff. All staff potentially working with whistleblowers should be made aware of the heightened information security concerns related to whistleblower information and be oriented to the practices, procedures, and protocols the office has in place to protect that information. It is advisable that offices incorporate the following considerations into staff planning and training:

(1) Every office should consider having a designated individual to serve as the principal contact for overseeing and implementing the policies concerning sensitive whistleblower information.

(2) All staff should be informed and educated of their responsibility for protecting sensitive whistleblower information, including the mandate to maintain whistleblower confidentiality in accordance with the House Code of Official Conduct.

i) This training can also be an opportunity to increase staff awareness of the whistleblower's rights concerning the information they provide to the office. These include the:

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

[5] Consult the House Office of Cybersecurity.

- Right to be informed about the collection of the sensitive information before the information is collected;
- Right to have the integrity and security of the information adequately protected;
- Right to review the information;
- Right to update the information and to correct errors;
- Right to request that information be deleted; and
- Right to object to the use of the information.

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.
- House Information Security Policy for the Protection of Sensitive Information, HISPOL 010.0, https://housenet.house.gov/technology/policies-and-standards/house-it-security-policies?utm_source=hn&utm_medium=web&utm_campaign=sm-tech.
- The House's comprehensive set of guidelines and supporting documents to address information security requirements can be found at: https://housenet.house.gov/technology/policies-and-standards.
- **Office of House Security**, http://sgtatarms.house.gov/ohs/ (for questions concerning handling of classified information).
- Clause 21 of Rule XXIII**, House Code of Official Conduct** (part of House Resolution 8, 117th Congress, Jan. 4, 2021), 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.

- **Impact Assessments:** The Privacy Impact Assessment (PIA) may be found in Section 208 of the E-Government Act of 2002, P.L. 107-347, 116 Stat. 2899 (Dec. 17, 2002), https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf, and the Office of Management and Budget (OMB) elaborated on the PIA in Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," (Sept. 26, 2003), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf.
- The Federal Trade Commission's **Fair Information Practice Principles** (FIPPS) are described in "Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress", Federal Trade Commission (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.
- The Federal Information Security Management Act of 2002 (**FISMA**) provides a comprehensive framework for ensuring information security. See Title III of the E-Government Act of 2002, P.L. 107-347, 116 Stat. 2899 (Dec. 17, 2002), https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf.
- The Cybersecurity and Infrastructure Agency (**CISA**) has a "Cyber Essentials" webpage for other steps toward cyber readiness: https://www.cisa.gov/cyber-essentials.