U.S. OFFICE OF SPECIAL COUNSEL
1730 M Street, N.W., Suite 218
Washington, D.C. 20036-4505
202-804-7000

February 1, 2018

MEMORANDUM FOR EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Henry J. Kerner, Special Counsel
U.S. Office of Special Counsel (OSC)

SUBJECT: Non-Disclosure Policies, Forms, or Agreements

This memorandum serves as an update to a 2013 memorandum on non-disclosure policies, forms, or agreements.[1] Five years ago, the Whistleblower Protection Enhancement Act of 2012 (WPEA) strengthened protections for federal employees who disclose suspected waste, fraud, or abuse. In addition, the WPEA modified rules on the use of non-disclosure policies, forms, or agreements by government agencies. Agencies should ensure that all non-disclosure policies, forms, or agreements conform to the WPEA's requirements, as detailed below. If you have questions about these provisions, please contact OSC.[2]

1. Agencies must include the notification statement required by the WPEA in all non-disclosure policies, forms, or agreements.

The WPEA amended section 2302(b) of Title 5, making it a prohibited personnel practice to implement or enforce any non-disclosure policy, form, or agreement, if such policy, form, or agreement does not contain the following statement:

> These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights,

[1] U.S. Office of Special Counsel, Memorandum for Executive Departments and Agencies, *The Whistleblower Protection Enhancement Act of 2012 and Non-Disclosure Policies, Forms, and Agreements* (Nov. 27, 2012), *available at* https://osc.gov/Resources/OSC%20Memorandum%20on%20Whistleblower%20Law%20and%20Non%20Disclosure%20Agreements%2003%2014%2013.pdf.

[2] This memorandum is intended to assist agencies in understanding and implementing the WPEA's requirements but is not an advisory opinion. Under 5 U.S.C. § 2302(d), OSC assists agencies in educating the federal workforce about whistleblower rights and protections and prohibited personnel practices. The WPEA's prohibitions and requirements are subject to interpretation by the Merit Systems Protection Board and the courts, where applicable.

> sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

This provision mirrors a longstanding appropriations restriction, which indicates that no funds may be used to implement or enforce any policy, form, or agreement lacking the required statement.[3] Accordingly, this statement should be incorporated into every non-disclosure policy, form, or agreement used by an agency.[4] While the WPEA does not define a non-disclosure policy, form, or agreement, Standard Form 312 (SF 312) is an example of a non-disclosure agreement. SF 312 restricts disclosure of classified information and states that failure to adhere to the restrictions in the agreement may result in the termination of a security clearance.[5] The Office of the Director of National Intelligence has updated SF 312 to add language that is compliant with the WPEA.

In the case of non-disclosure policies, forms, or agreements in effect before the WPEA's effective date (December 26, 2012), the law allows agencies to continue to enforce a policy, form, or agreement that does not contain the statement if the agency gives an employee notice of the statement. Agencies may cure a non-complying non-disclosure policy, form, or agreement with an email to agency employees, and thereby avoid the need to reissue non-disclosure agreements. Below is a sample email that agencies may choose to issue to employees:

> *Dear Employee:*
>
> *The Whistleblower Protection Enhancement Act of 2012 (WPEA) was signed into law in 2012. The law strengthened the protections for federal employees who disclose evidence of waste, fraud, or abuse. The WPEA also requires that any non-disclosure policy, form, or agreement include the statement copied below, and provides that any such policy, form or agreement executed without the language may be enforced as long as agencies give employees notice of the statement. This communication serves as that notice to employees.*
>
> *As a XXX Department employee, you may have been required to sign a non-disclosure policy, form, or agreement to access classified or other information. You should read this statement as if it were incorporated into any non-disclosure policy, form, or agreement you have signed.*

---

[3] *See, e.g.,* Consolidated Appropriations Act, 2017, Pub. L. 115-31 Div. E § 744, 131 Stat. 135, 389 (2017).

[4] Please note that section 104 of the WPEA, which makes it a prohibited personnel practice to implement or enforce a non-disclosure policy, form, or agreement without the required statement, does not apply to the intelligence community elements listed in 5 U.S.C. § 2302(a)(2)(C)(ii). However, Section 115 of the WPEA, which requires that non-disclosure policies, forms, and agreements contain the whistleblower rights notice discussed above, applies government-wide, as does the aforementioned appropriations restriction.

[5] Agencies may distinguish between a non-disclosure policy, form, or agreement and a confidentiality clause in a settlement agreement. A confidentiality clause in a settlement agreement is not covered by the WPEA's notice requirements if it only restricts disclosure of the terms and conditions of the settlement. If a confidentiality clause in a settlement agreement extends beyond those terms and conditions to restrict disclosure of any other information, agencies must incorporate the WPEA's statement.

These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

Employees are reminded that reporting evidence of waste, fraud, or abuse involving classified information or classified programs must continue to be made consistent with established rules and procedures designed to protect classified information.

In the case of former employees who are covered by the terms of a non-disclosure policy, form, or agreement, an agency may continue to enforce such agreements if it posts the required statement on its web site, as detailed below.

2. Agencies should update their web sites by posting the required statement and a list of controlling Executive orders and statutory provisions.

The WPEA further requires that agencies making use of any non-disclosure policy, form, or agreement post the WPEA statement noted above on the agency website, accompanied by the specific list of controlling Executive orders and statutory provisions. As noted above, in the case of former employees who are covered by the terms of a non-disclosure policy, form, or agreement, agencies may continue to enforce such agreements if the agency posts the required statement on its website. Accordingly, agencies should post the required statement on a publicly accessible web page and may also choose to post on an internal web page.

In addition, agencies should post the following list of Executive orders and statutory provisions, and clarify that these provisions are controlling in the case of any conflict with an agency non-disclosure policy, form, or agreement:

- Executive Order No. 13526;
- Section 7211 of Title 5, United States Code (governing disclosures to Congress);
- Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military);
- Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats);
- Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents);
- The statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, and 952, of title 18, United States Code; and

- Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)).

Last, OSC urges agencies to be mindful of the guidelines discussed above when they educate employees about any information security or communication requirements or restrictions. Even if these materials are not non-disclosure policies, forms, or agreements, agencies should not convey information in a way that may have a chilling effect on lawful whistleblowing. Rather, agencies should develop guidance, including guidance related to insider threat programs, with the following whistleblower protections in mind:

- Except where required by law, whistleblowers need not make disclosures through any particular channel.[6] There are many permissible ways for a whistleblower to make disclosures, *e.g.*, to OSC, to an IG, to agency leadership, to officials outside the employee's chain of command, to Congress, or to the media.

- Disclosures are protected unless they are specifically prohibited by law or Executive order.[7] Although materials that agencies circulate to employees may use phrases such as "unauthorized disclosures," "leak," or "leakers," these terms can be ambiguous and may cause employees to believe that lawful whistleblowing activities are being curtailed. Employees who make protected disclosures have not "leak[ed]" information, nor are they "leakers." Therefore, agencies should be mindful about the use of such terms. In cases where agencies use the term "unauthorized disclosures" to refer to those specifically prohibited by law, a clear distinction should be drawn between this term and protected whistleblowing. To ensure that employees understand the scope of the prohibition agencies mean to convey when addressing "unauthorized disclosures," a best practice would be to carefully define this term so that it pertains only to the disclosure of information that is prohibited by law or Executive order. Agencies should also communicate the appropriate process for making disclosures about this type of information.

---

[6] Under section 2302(b)(8), employees do not have to use a particular channel to make a disclosure if such disclosure "is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs." Where this statutory exception applies, as it would in the case of classified information, employees must utilize specific channels when making a disclosure. These channels are OSC, IGs, and "another employee designated by the head of the agency to receive such disclosures." *Id.; see also* National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91 § 1097(b) (requiring agency heads to ensure that employees are informed of the means by which they may lawfully disclose classified information to OSC, inspectors general, Congress, or designated agency officials).

[7] 5 U.S.C. § 2302(b)(8).