



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

SUBJECT: Agency Monitoring Policies and Whistleblower Disclosures

This memorandum serves as an update to a 2012 memorandum that identified certain legal restrictions and guidelines agencies should consider when evaluating their policies and practices about monitoring employee communications.¹ Although lawful agency monitoring of employee communications serves legitimate purposes, federal law also protects the ability of workers to exercise their legal rights to disclose wrongdoing without fear of retaliation. Indeed, federal employees are required to disclose waste, fraud, abuse, and corruption to appropriate authorities² and are expected to maintain concern for the public interest,³ which may include disclosing wrongdoing.

OSC strongly urges executive departments and agencies (agencies) to evaluate their monitoring policies and practices, and take measures to ensure that these policies and practices do not interfere with or chill employees from lawfully disclosing wrongdoing. The following legal restrictions and guidelines should be considered as part of this evaluation.

Legal Framework

Federal law generally prohibits personnel actions taken, not taken, or threatened against a federal employee because of the employee's disclosure of information that he or she reasonably believes evidences a violation of any law, rule, or regulation, or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.⁴ In addition, an employee's right to "furnish information to either House of Congress, or to a committee or Member thereof, may not be interfered with or denied."⁵ Subject to certain

¹ U.S. Office of Special Counsel, Memorandum for Executive Departments and Agencies, *Agency Monitoring Policies and Confidential Whistleblower Disclosures to the Office of Special Counsel and to Inspectors General* (June 20, 2012), available at https://osc.gov/Resources/omb_and_osc_memos_on_agency_monitoring_policies.pdf.

² See Ethics Principle No. 11, 5 C.F.R. § 2635.101(b)(11).

³ See Merit Principle No. 4, 5 U.S.C. § 2301(b)(4).

⁴ See 5 U.S.C. § 2302(b)(8).

⁵ 5 U.S.C. § 7211. This provision of the Lloyd-LaFollette Act of 1912 was given further effect through an appropriations restriction in place since Fiscal Year 1998, found most recently in the Consolidated Appropriations Act, 2017, Pub. L. No. 115-31 Div. E § 713, 131 Stat. 135, 379 (2017). The provision states:

exceptions, federal law also protects the identity of an employee who makes such a protected disclosure to OSC or an agency inspector general (IG).⁶

Guidelines

Agency monitoring specifically designed to target protected disclosures may be unlawful, as it undermines the ability of employees to make confidential disclosures. Moreover, deliberate targeting by an employing agency of an employee's submission (or draft submissions) to OSC or IGs, or deliberate monitoring of communications between the employee and OSC or IGs in response to such a submission by the employee, could lead to OSC determining that the agency has retaliated against the employee for making a protected disclosure.

The risk that agency monitoring will discourage protected whistleblowing is not limited to contact with OSC or IGs, as employees may disclose most types of information outside of these channels, *e.g.*, to agency leadership, to officials outside their chain of command, to Congress, or to the media. Monitoring an employee's communications, including emails, computer files, or conversations, simply because the employee made or may make a protected disclosure has a chilling effect on these lawful activities.

OSC recognizes that agencies have a legitimate interest in protecting information that cannot legally be disclosed outside of prescribed channels, such as classified materials. Efforts to educate employees about their responsibilities in this area are necessary and important. However, agencies must strike a balance between safeguarding these types of information and discouraging protected disclosures. In this vein, employees should not be reported for making lawful disclosures, as this creates a false impression that they have engaged in misconduct. Moreover, reporting whistleblowers may suggest that they are being tracked by their agencies. Both of these circumstances discourage employees from making protected disclosures and impede efforts to reduce government waste, fraud, and abuse.

No part of any appropriation contained in this or any other Act shall be available for the payment of the salary of any officer or employee of the Federal Government, who—

- (1) prohibits or prevents, or attempts or threatens to prohibit or prevent, any other officer or employee of the Federal Government from having any direct oral or written communication or contact with any Member, committee, or subcommittee of the Congress in connection with any matter pertaining to the employment of such other officer or employee or pertaining to the department or agency of such other officer or employee in any way, irrespective of whether such communication or contact is at the initiative of such other officer or employee or in response to the request or inquiry of such Member, committee, or subcommittee; or
- (2) removes, suspends from duty without pay, demotes, reduces in rank, seniority, status, pay, or performance or efficiency rating, denies promotion to, relocates, reassigns, transfers, disciplines, or discriminates in regard to any employment right, entitlement, or benefit, or any term or condition of employment of, any other officer or employee of the Federal Government, or attempts or threatens to commit any of the foregoing actions with respect to such other officer or employee, by reason of any communication or contact of such other officer or employee with any Member, committee, or subcommittee of the Congress as described in paragraph (1).

⁶ See 5 U.S.C. § 1213(h) (prohibiting the Special Counsel from disclosing the identity of a whistleblower without the individual's consent unless disclosure becomes necessary due to an imminent danger to public health or safety or imminent violation of any criminal law); Inspector General Act of 1978, 5 U.S.C. App. § 7(b) (prohibiting IGs from disclosing the identity of a whistleblower without the whistleblower's consent unless an IG determines such disclosure is unavoidable during the course of an investigation).

Summary

In sum, we strongly recommend that agencies review existing monitoring policies and practices, including insider threat program information, to ensure that they are consistent with both the law and Congress's intent to encourage protected disclosures.

CHAIRMAN Resource

From: U.S. Office of Special Counsel <2302c@osc.gov>
Sent: Thursday, February 01, 2018 2:44 PM
To: Wall, Ashley
Subject: [External_Sender] OSC's Special Counsel Issues Three Memoranda to Agency Heads and Inspectors General
Attachments: 2018 Agency Requirements Memo.pdf; NDA Memo Update.pdf; Agency Monitoring Memo Update.pdf

On February 1, 2018, Special Counsel Henry J. Kerner issued a guidance memorandum on the new statutory requirements regarding agency training and discipline. He has also updated two previously issued memoranda on a) agency monitoring policies and whistleblower disclosures and b) non-disclosure policies, forms, or agreements. All three memoranda are attached to this email.

Notably, the first memorandum requires agencies to take active steps, in consultation with the Office of Special Counsel (OSC), to modify and enact training and education provisions with respect to prohibited personnel practices, including whistleblower retaliation, and establish new disciplinary requirements. These new requirements are the result of two pieces of legislation the President signed into law at the end of 2017: the Dr. Chris Kirkpatrick Whistleblower Protection Act of 2017 and the Office of Special Counsel Reauthorization Act of 2017. The second and third memoranda urge departments and agencies to ensure that their non-disclosure policies, forms, and agreements conform to statutory requirements, and that their monitoring policies and practices (including insider threat program information) do not interfere with or chill employees from lawfully disclosing wrongdoing. OSC's guidance should be used in that evaluation.

We would like to acknowledge your agency for its previous efforts in certifying and/or registering for OSC's Certification Program. Your agency has already taken many of the steps needed to educate your workforce on employee rights and responsibilities under the civil service and whistleblower protection laws. The new requirements will further enhance your agency's ability to foster an open culture where legitimate concerns are addressed and wrongdoing is prevented.

We encourage you to have a member of your staff contact Shirine Moazed, Chief, Diversity, Outreach, and Training (DOT), and Ashley Wall, DOT's Program Coordinator, at (202) 804-7163 or certification@osc.gov. The DOT staff will be able to assist your [certification program agency liaison](#) with the new requirements and ensure that any other questions you may have will be answered by the appropriate experts here at OSC. If you have questions not related to training and certification, please call (202) 804-7000.

Please confirm your receipt of this email to the above email, certification@osc.gov.

NOTICE: This message and any attachments may contain information that is sensitive, confidential, or legally privileged. If you are not the intended recipient, please immediately notify the sender and delete this email from your system; you should not copy, use, or disclose its contents. Thank you for your cooperation.