EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 20, 2012

MEMORANDUM FOR CHIEF INFORMATION OFFICERS AND GENERAL COUNSELS

FROM: Steven VanRoekel
Federal Chief Information Officer

Boris Bershteyn
General Counsel

SUBJECT: Office of Special Counsel Memorandum on Agency Monitoring Policies and Confidential Whistleblower Disclosures

The attached memorandum from the Office of Special Counsel (OSC) identifies certain legal restrictions and guidelines that executive departments and agencies should consider when evaluating their policies and practices regarding monitoring of employee electronic mail and other communications. 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, which is essential to good government.

We strongly urge you to carefully review the attached OSC memorandum when evaluating your agency's monitoring policies and practices, and to take appropriate steps to ensure that those policies and practices do not interfere with or chill employees' use of appropriate channels to disclose wrongdoing.

U.S. OFFICE OF SPECIAL COUNSEL
1730 M Street, N.W., Suite 218
Washington, D.C. 20036-4505
202-254-3600

June 20, 2012

MEMORANDUM FOR EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Special Counsel Carolyn N. Lerner
U.S. Office of Special Counsel

SUBJECT: Agency Monitoring Policies and Confidential Whistleblower Disclosures to the Office of Special Counsel and to Inspectors General

This memorandum identifies certain legal restrictions and guidelines that agencies should consider when evaluating their policies and practices regarding monitoring of employee electronic mail and other communications. 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, which is essential to good government. Indeed, Federal employees are required to disclose waste, fraud, abuse, and corruption to appropriate authorities[1] and are expected to maintain concern for the public interest,[2] which may include disclosing wrongdoing.

We strongly urge 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 using appropriate channels to disclose wrongdoing. The following legal restrictions and guidelines should be considered as part of this evaluation.

Legal Framework

Federal law generally prohibits adverse personnel actions against a Federal employee because of an employee's disclosure of information that the employee 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.[3] Subject to certain exceptions, Federal law also protects the identity of an employee who makes

---

[1] *See* Ethics Principle No. 11, 5 C.F.R. § 2635.101(b)(11).

[2] *See* Merit Principle No. 4, 5 U.S.C. § 2301(b)(4).

[3] *See* 5 U.S.C. § 2302(b)(8).

such a protected disclosure to the Office of Special Counsel (OSC) or an agency Inspector General (IG).[4]

Guidelines

In light of this legal framework, agency monitoring specifically designed to target protected disclosures to the OSC and IGs is highly problematic. Such targeting 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 the OSC or an IG, or deliberate monitoring of communications between the employee and the OSC or IG in response to such a submission by the employee, could lead to a determination that the agency has retaliated against the employee for making a protected disclosure. The same risk is presented by an employing agency's deliberate targeting of an employee's emails or computer files for monitoring simply because the employee made a protected disclosure.

Summary

In sum, we strongly recommend that agencies review existing monitoring policies and practices to ensure that they are consistent with both the law and Congress's intent to provide a secure channel for protected disclosures.

[4] *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); 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).