




U.S. Department of Justice
Justice Management Division

Washington, D.C. 20530

POLICY MEMORANDUM # 2018-02

DATE: September 11, 2018

TO: All Department of Justice (DOJ) Components

FROM: Lee J. Lofthus
Assistant Attorney General for Administration
Justice Management Division 

SUBJECT: DOJ Order 2740.1A, *Use and Monitoring of Department of Justice Computers and Computer Systems*

PURPOSE: This Policy Memorandum cancels sections 3.f., and 3.g., of DOJ Order 2740.1A. The below language is now substituted for these cancelled provisions. This substituted language is the mandated policy under DOJ Order 2740.1A.

f. **Monitoring, Disclosing, or Accessing Email or Documents on Computer Systems.** Use of departmental computer systems constitutes consent to monitoring and disclosure of information stored on or transiting the departmental computer system. The Department routinely conducts monitoring and intercepts communications for security purposes and to detect improper use. Such monitoring and interception includes the use of software tools that examine the content of Internet communications and email, and block access to known or suspected malicious Internet sites. The Department may block or otherwise prevent any improper use or activity prohibited in section 3.c. above.

(1) **Accessing an Employee's or Contractor's Electronic Information.** Monitoring, disclosing, and accessing another employee's or contractor's email messages, Internet activities, documents, files, or other information stored on or transiting the departmental computer system may only be done in compliance with this Order. Accessing shared storage (i.e., a server or disk drive intended for shared or public access) or accessing emails pursuant to sharing permissions does not constitute accessing another employee's or contractor's information.

(2) **Component Designated Officials' Responsibilities**

(a) The Heads of Department Components shall designate officials responsible for reviewing and approving, in their discretion, the monitoring, disclosing, or accessing of the electronic information of employees or contractors in their respective component only, except as otherwise provided in this Order, for the permitted purposes listed in section f(4). Designated officials must be at the Assistant Director level or higher for bureaus, and at the Chief of Staff or Deputy Director level or higher for the Offices, Boards, and Divisions. The component shall notify the Assistant Attorney General for Administration (AAG/A) of this designation.

(b) Any requests that the Justice Management Division (JMD) receives for access to the information of another component's employees or contractors for the permitted purposes listed in section f(4) will be referred to the component designated official, except in the limited circumstances specified in section f(5).

(3) **Permitted Purposes for Monitoring, Disclosing, or Accessing Electronic Information Not Requiring Approval by the Designated Official.**

(a) System managers and information technology security personnel may engage in routine system administration and system security monitoring in accordance with applicable

policies and procedures without seeking approval under this Order. Routine system administration does not include targeted, direct access to an employee's or contractor's mailbox or files, or targeted searches of the information of individuals or groups of individuals.

- (b) Potentially improper activities detected pursuant to routine system administration and system security monitoring must be reported to the appropriate component and to Department authorities as necessary. Use of such information by the recipient of such reports for official purposes, including disciplinary purposes, does not require approval under this Order. The component involved should be notified of such subsequent use to the extent practicable.
 - (c) In order to prevent death or serious injury to any person.
- (4) **Permitted Purposes for Monitoring, Disclosing, or Accessing Information Requiring Advance Approval by the Designated Official**

The officials designated in Section f(2) may approve monitoring, disclosing, or accessing information in an employee's or contractor's computer system for the following purposes:

- (a) For investigatory purposes by, or as authorized by the Office of Professional Responsibility of the Department or of a component, the Office of the Inspector General, the Federal Bureau of Investigation, or the Criminal Division (in the context of a criminal investigation).
- (b) An insider threat inquiry as authorized by Department policy.
- (c) In response to a court order, grand jury subpoena, or search warrant.
- (d) In response to a Freedom of Information Act (FOIA) or Privacy Act (PA) request, for the purpose of responding to the FOIA or PA request, with notice to the employee or contractor whose email messages or other information is being accessed. Where the request concerns a former employee or contractor of the component, notice to the individual is not required before approving access for this purpose.
- (e) Accessing an employee's or contractor's email messages or other information when necessary for business purposes, with notice to the employee or contractor. In the case of a former employee or contractor of the component, notice is not required in order to approve access for this purpose. A business purpose

includes accessing a needed file during an employee's or contractor's illness or absence, but does not include investigating suspected misconduct.

- (f) In response to a litigation hold or a discovery request, granting access for attorneys or other employees for the purpose of complying with litigation requirements, with notice to the employee or contractor whose email messages or other information is being accessed. In the case of a former employee or contractor of the component, notice is not required in order to approve access for this purpose.

(5) **Limited Role of JMD as System Manager in Shared Service Environment.** JMD will not act on but rather will refer any requests it receives for access to the information of another component's employees or contractors for the purposes listed under section f(4) to the component designated official, except in the following limited circumstances:

- (a) Where the request is for access to the records of an Assistant Director or higher, with prior notice to the Head of Component, unless he or she is subject to the request, with written approval by the Office of the Deputy Attorney General (ODAG);
- (b) Where directed by the investigating or authorizing office to conduct the search without notifying the component, with receipt of the request documented, and with written approval by the ODAG;
- (c) For Department-wide or multi-component searches, with prior notice to the components, and with written approval by the ODAG.

Disclosure shall be made to a designated official for the component(s) in question within 5 business days after the conditions for non-disclosure are removed.

(6) **Other Purposes Requiring Special Authorization**

Access to an employee's or contractor's electronic information for any other reason, including suspected misconduct not connected with a permitted purpose in section f(3) or f(4), must be authorized by:

- (a) The Head of the Bureau (as defined in 28 C.F.R. § 0.1) where the employee works, for Bureau personnel;
- (b) The Head of the Executive Office for U.S. Attorneys, for U.S. Attorneys personnel;
- (c) The Head of the Executive Office for U.S. Trustees (EOUST),

for EOUST personnel;

- (d) The AAG/A for all other components.

This authority may not be delegated below the Assistant Director level or equivalent.

- (7) **Notification of and Consent to Monitoring and Disclosure.** All components are required to provide adequate notice to their employees and contractors that their use of the departmental computer system constitutes consent to monitoring and disclosure. The Standard Warning Banner promulgated by the Department's Chief Information Officer provides such adequate notice.

- g. **Employee Activities.** Nothing in this policy creates any enforceable rights. Unauthorized use or monitoring or improper access to an employee's computer system may result in disciplinary action or criminal prosecution. Employees and contractors are prohibited from accessing the email, electronic files or documents, or otherwise monitoring the online activities of another employee or contractor except in accordance with this policy.
- h. **Sanctions for Misuse.** Unauthorized or improper use of Department office equipment could result in loss of use or limitations on use of equipment, disciplinary or adverse actions, and/or criminal penalties.