DOJ 2740.1A Change 1

USE AND MONITORING OF DOJ COMPUTERS AND COMPUTER SYSTEMS

Approval Date: November 30, 2010

Approved By: Lee J. Lofthus
Assistant Attorney General
for Administration

Initiated by: Justice Management Division
Office of General Counsel

1. **PURPOSE.** This Order states the Department's policy on the use of departmental computers and computer systems, the lack of expectation of privacy with respect to such use, and authorized monitoring or access to information on departmental computers and computer systems.

2. **SCOPE.** This policy applies to all classified and unclassified computer systems and peripheral devices (such as Personal Electronic Devices) that are acquired for use by, owned, operated, or managed by a departmental component. A privately-owned computer or device that is connected to a departmental computer system is considered to be a departmental computer system while so connected. This policy applies to all Department components.

3. **POLICY.**

   a. **Approval for Deviation from Policy.** No component shall issue any less restrictive policy with respect to the acceptable and prohibited use of Department computer systems and Department provided Internet resources without written approval of the Department's Chief Information Officer. Components may issue further implementation guidance on such use consistent with this policy without written approval. Components may not deviate from the monitoring and access provisions of this Order.

b. **Use of Department Computers and Computer Systems.**

(1) Use of departmental computer systems, including but not limited to Internet e-mail, departmental e-mail, word processing systems, and connections to Internet sites, is subject to the same restrictions on use as are other government-furnished resources provided for the use of employees. (See 5 C.F.R. § 2635.101(b)(9) and 2635.704.)

(2) While departmental computer systems are provided for official use, some personal use of government computer systems is permitted in accordance with existing policy on personal use of government property, where there is negligible cost to the government and no interference with official business. (See 28 C.F.R. § 45.4.)

c. **Prohibited Use of Department Computers and Computer Systems.**

(1) The following activities are prohibited on department computers and computer systems during working or nonworking hours:

(a) Downloading and/or installing any program, software or executable file on department computers, unless approved in accordance with component IT security policy.

(b) Non-official use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, electronic greeting cards, video, sound or other large file attachments can degrade the performance of the entire network, and should not be viewed or sent on Department computers. Accessing continuous data streams (such as viewing streaming video or listening to streaming audio/radio on a media website) could also degrade the performance of the entire network and is inappropriate when not for official purposes.

(c) Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).

(d) Sending out solicitations, participating in any lobbying activity, or engaging in prohibited political activity

(e) Unauthorized use for posting agency information to external newsgroups, bulletin boards or other public forums. This includes: any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee without appropriate Agency approval, or uses at odds with the agency's mission or positions.

(2) The following activities are prohibited on department computers and computer systems during working or non-working hours, except when conducting legitimate departmental business with the express prior permission of the employee's Component Head, Deputy Component Head or Field Office Head:

(a) Use of Internet sites that result in an additional charge to the government.

(b) Using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

(c) The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials or materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities.

(d) Any use to circumvent security controls on Department or other external systems.

(e) Knowingly using anonymizer sites (anonymizer sites hide the user's identity from the Internet site being visited; however, in doing so, they also bypass the blocking mechanism designed to protect Department systems from malicious Internet sites).

(f) Knowingly visiting malicious resources or sites.

(g) Using peer-to-peer (P2P) file sharing sites on the Internet (e.g., sites dedicated to downloading audio or video files), or using IP telephony sites.

(h) Any otherwise prohibited activity.

d. **Proper Representation** It is the responsibility of employees to ensure that they are not giving the false impression that they are acting in an official capacity when they are using government office equipment for nongovernment purposes. If there is expectation that such a personal use could be interpreted to represent an agency, then an adequate disclaimer must be used. One acceptable disclaimer is - "The contents of this message are mine personally and do not reflect any position of the Government or my agency." The Standards of Conduct states - "…an employee shall not use or permit the use of his Government position or title or any authority associated with his public office in a manner that could reasonably be construed to imply that his agency or the Government sanctions or endorses his personal activities…" (5 CFR § 2635.702(b)).

e. **No Expectation of Privacy.** Individual employees and contractors should NOT expect privacy in the use of government computers or computer systems. The Department may access e-mail messages, files, records, or other documents on government computer systems

whenever it has a legitimate governmental purpose for doing so.

f. **Monitoring, Disclosing, or Accessing E-mail 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 as provided below. 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) **Authorized Access.** Monitoring, disclosing, and accessing another employee's or contractor's e-mail messages, Internet activities, documents, files, or other information stored on or transiting the departmental computer system may only be done for authorized purposes. Accessing shared storage (i.e., a server or disk drive intended for shared or public access) or accessing e-mails pursuant to sharing permissions does not constitute accessing another employee's or contractor's computer system.

(2) **Authorized Purposes for Monitoring, Disclosing, or Accessing:**

(a) For system administration and system security.

(b) Improper activities detected pursuant to system administration and system security may be reported to the appropriate component and Department authorities. Use of such information by the recipient of such reports for official purposes, including disciplinary purposes, constitutes an authorized purpose.

(c) For investigatory purposes by, or as authorized by, the Office of Professional

Responsibility, the Office of the Inspector General, the Federal Bureau of Investigation, or the Criminal Division.

(d) In response to a court order, grand jury subpoena, or search warrant.

(e) In response to a Freedom of Information Act (FOIA) or Privacy Act (PA) request, a system manager may provide access to FOIA/PA professionals, attorneys, or other designated employees for the purpose of responding to the FOIA or PA request with notice to the employee or contractor whose e-mail messages or other information is being accessed. In the case of a former employee or contractor, notice is not required in order to provide access for this purpose.

(f) At the request of a component head, deputy component head, or assistant bureau director, a system manager may provide access to an employee's or contractor's e-mail 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, notice is not required in order to provide 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.

(g) In response to a litigation hold at the outset of civil litigation against the Department whether actual or reasonably anticipated or a discovery request, a system manager may provide access to attorneys or other designated employees for the purpose of complying with litigation requirements with notice to the employee or contractor whose e-mail messages or other information is being accessed. In the case of a former employee or contractor, notice is not

required in order to provide access for this purpose.

(h) In order to prevent death or serious injury to any person.

(3) **Authorizing Officials.** Access to an employee's computer system for any other reason, including suspected misconduct not detected in the course of system administration and not connected with an official investigation by one of the offices listed above, must be authorized by:

(a) The head of the Bureau (as defined in 28 CFR § 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 head of the National Drug Intelligence Center (NDIC), for NDIC personnel; or

(e) The Assistant Attorney General for Administration for all other components.

This authority may not be delegated below the level of a principal deputy.

(4) **Notification of 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.

(5) **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 e-

mail, electronic files or documents, or otherwise monitoring the online activities of another employee or contractor except in accordance with this policy.

g. **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.

/s/ Lee J. Lofthus
Assistant Attorney General
for Administration