



## **MILITARY AND DoD CIVILIAN EMPLOYEE STANDARDS OF CONDUCT**

### **On the Official Use and Authorized Purposes of Federal Government Resources (Communication Systems)**

If you need advice on a particular situation please contact MCLB SJA at (229) 639-5212 or LOGCOM Office of Counsel at (229) 639-7098 or by email at [Office of Counsel](#) to set up an appointment with one of the attorneys.

*References:* DODD 5500.07; JER DOD 5500.7-R

This handout provides a synopsis of the official use and authorized purposes of the Federal Government resources, namely the communications systems, including the punitive or adverse administrative nature for any violation, and the applicable excerpts from the Joint Ethics Regulation – as it applies to both military members and DoD civilian employees.

**NOTE:** Pursuant to paragraph 2.2.6.1 of Department of Defense Directive 5500.07 (Standards of Conduct) the provisions printed in bold italics in DoD 5000.7-R (Joint Ethics Regulation (JER)), constitute lawful general orders within the meaning of the Uniform Code of Military Justice (UCMJ), are punitive, and apply without further implementation. In addition, violation of any provision of the JER may constitute the UCMJ offense of dereliction of duty or other punitive article. **Per 2.2.6.2 of DODD 5500.07, violation of any provision of the JER, by DoD civilians** may result in appropriate criminal prosecution, civil judicial action, disciplinary or adverse administrative action, or other administrative action authorized by U.S.C. or Federal regulations.

2-301. Use of Federal Government Resources.

a. Communication Systems. See GSA regulation 41 C.F.R. Subpart 201-21.6 (reference (h)) on use of Federal Government telephone systems. ***Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only.***

(1) Official use includes emergency communications and communications that the DoD Component determines are necessary in the interest of the Federal Government. Official use may include, when approved by theater commanders in the interest of morale and welfare, communications by military members and other DoD employees who are deployed for extended periods away from home on official DoD business.

(2) Authorized purposes include brief communications made by DoD employees while they are traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DoD employee's usual work place that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief internet searches; e-mailing directions to visiting relatives) when the Agency Designee permits categories of communications, determining that such communications:

(a) Do not adversely affect the performance of official duties by the DoD employee or the DoD employee's organization;

(b) Are of reasonable duration and frequency, and whenever possible, made during the DoD employee's personal time such as after duty hours or lunch periods;

(c) Serve a legitimate public interest (such as keeping DoD employees at their desks rather than requiring the use of commercial systems; educating the DoD employee on the use of the communications system; improving the morale of DoD employees stationed for extended periods away from home; enhancing the professional skills of the DoD employee; job-searching in response to Federal Government downsizing);

(d) Do not put Federal Government communications systems to uses that would reflect adversely on DoD or the DoD Component (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service); and

(e) Do not overburden the communication system (such as may be the case with broadcasts and group mailings), create no significant additional cost to DoD or the DoD Component, and in the case of long distance communications, charges are:

1 Charged to the DoD employee's home telephone

number or other non-Federal Government number (third number call);

2 Made to a toll-free number;

3 Reversed to the called party if a non-Federal Government number (collect call);

4 Charged to a personal telephone credit card; or

5 Otherwise reimbursed to DoD or the DoD Component in accordance with established collection procedures;

**(3) *In accordance with applicable laws and regulations, use of Federal Government communications systems may be monitored. See DoD Directives 4640.1 (reference (i)) and 4640.6 (reference (j)). DoD employees shall use Federal Government communications systems with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.*** In addition, use of such systems is not anonymous. For example, for each use of the internet over Federal Government systems, the name and computer address of the DoD employee user is recorded by the Government and also by the locations searched.

**(4) *Most Federal Government communications systems are not secure. DoD employees shall not transmit classified information over any communication system unless it is transmitted using approved security procedures and practices (e.g., encryption, secure networks, secure workstations). In addition, DoD employees shall not release access information, such as passwords, to anyone unless specifically authorized to do so by the Agency Designee. See DoD Directives 5200.28 (reference (k)) and C-5200.5 (reference (l)). DoD employees should exercise extreme care when transmitting any sensitive information, or other valued data. Information transmitted over an open network (such as through unsecure e-mail, the internet, or telephone) may be accessible to anyone else on the network. Information transmitted through the internet or by e-mail, for example, is accessible to anyone in the chain of delivery. Internet information and e-mail messages may be re-sent to others by anyone in the chain.***