DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DISA INSTRUCTION 630-225-15* 12 Sep 14

INFORMATION SERVICES

Authorized Unofficial Use of Government-Provided Information Technology (IT)

1. **Purpose.** This Instruction prescribes policy, implements departmental guidance, and assigns responsibilities for authorized unofficial use of government-provided information technology (IT).

2. **Applicability**. This Instruction applies to all DISA civilian, military, and contractor personnel accessing DISA information systems.

*3. **Authority.** This Instruction is published in accordance with the authority contained in DoD 5500.7-R, Joint Ethics Regulation (JER), August 1993, including changes through 17 November 2011, and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D, Defense Information Systems Network (DISN) Responsibilities, 24 January 2012.*

~~3.~~*4*. **Background.**

~~3~~*4.1* Taxpayers have the right to depend on their government to manage their tax dollars wisely and effectively. Public confidence in the productiveness of government is increased when members of the public are confident that their government is well managed and assets are used appropriately. Productivity increases have come about through the use of modern IT equipment and systems; such as, computers, scanning devices, and the Internet. These technologies provide new opportunities for employees to live their lives more efficiently, while balancing the overriding imperative that American taxpayers receive the maximum benefit for their tax dollars.

~~3~~*4.2* Agency personnel are recognized as responsible individuals who are the key to making government more responsive to its citizens. ~~It~~ *This Instruction* defines acceptable and unacceptable types of unofficial use of government-provided IT assets, which are accompanied with additional responsibilities for DISA personnel. ~~It~~ *This Instruction* in no way limits Agency personnel in the use of government-provided IT for official activities~~, consistent with existing protections of sensitive data.~~

~~4. References.~~

~~4.1 DoD 5500.7-R, Joint Ethics Regulation (JER), current version.~~

~~4.2 CJCSI 6211.02C, Defense Information System Network (DISN): Policy and Responsibilities, 9 July 2008.~~

~~4.~~*5.* **Definitions.**

~~4.~~*5.1* **Information Technology.** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, duplication, management, movement control, display, switching, interchange, transmission, or reception of data or information.

~~4.~~*5.2* **Minimal Additional Expense.** Employee authorized unofficial use of government-provided IT is limited to those situations where the government is already providing the IT and the employee's use of such equipment or services will not result in any significant additional expense to the government or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner, or paper. Examples of minimal additional expenses include making a few photocopies, using a computer printer to printout a few pages of material, sending personal e-mail messages, or limited use (infrequent and small use of bandwidth) of the Internet for personal reasons.

~~4.~~*5.3* **Employee Nonwork Time.** Times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use government-provided IT during off duty hours; such as, before or after their scheduled tour of duty, lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times).

~~4.~~*5.4* **Authorized Unofficial Use.** Use of government-provided equipment for personal purposes or communications ~~that does not violate the general restrictions of~~ *consistent with* the ~~references~~ *authority documents* or other DoD issuances. Such use includes personal communications from the employee's usual workplace that are most reasonably made while at the work place; such as, checking in with spouse or minor children; scheduling doctor, automobile, or home repair appointments; brief Internet searches; and personal e-mails. Employees may also check their Thrift Savings Plan or other personal investments or seek employment.

6. **Policy.**

6.1 It is DISA policy to provide its personnel with a professional supportive work environment. DISA personnel should be given the tools needed to effectively carry out their assigned responsibilities. Authorizing limited unofficial use of government-provided IT assets helps enhance the quality of the work place and helps the government retain highly qualified and skilled workers.

6.2 Consistent with the ~~references~~ *authority documents*, DISA personnel are permitted limited use of government-provided IT for personal needs if the use does not interfere with official business and *does not* involve~~s~~ ~~minimal~~ *significant* additional expense to the government. This limited personal use of government-provided IT should, *when reasonably possible,* take place during the employee's nonwork time. Authorized limited unofficial use of government-provided IT must not result in loss of personnel productivity or interference with official duties. The privilege never extends to modifying IT equipment, including loading personal software or making configuration changes. Authorized unofficial use of government-provided IT is a privilege that may be revoked or limited at any time by appropriate Agency officials.

6.3 Personnel will not use government-provided IT for activities prohibited by the ~~references~~ *authority documents*, any other DoD issuance, or the unauthorized uses cited in paragraph 8.

6.4 DISA officials shall apply this policy to contractor personnel and other nongovernment employees through incorporation by reference in contracts or memorandums of agreement as conditions for using government office equipment and space.

7. **General Limits on Consumption**. Unofficial use is *not* authorized ~~only~~ if it results in ~~minimal~~ *significant* additional expense to the government in areas such as communications bandwidth (e.g., e-mails with ~~either no or small~~ *large* attachments); use of consumables in ~~limited~~ *significant* amounts (e.g., paper, ink, toner, etc.); ~~general~~ *excessive* wear and tear on equipment; and ~~limited~~ *use of large* storage space on data storage devices.

8. **Unauthorized Use**. Unauthorized use of government-provided IT and/or office equipment that would adversely reflect on DISA, includes the following:

8.1 Any unofficial use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network. "Push" technology on the Internet and other continuous data streams; such as, commercial radio or television broadcasts or other unofficial audio or video services ~~would~~ *can* also degrade the performance of the entire network and, *if so, would* be an inappropriate use.

8.2 Using government systems as a staging ground or platform to gain unauthorized access to other systems.

8.3 The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.

8.4 Using government-provided IT for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

8.5 Use of government-provided IT to maintain or support a personal private business. Examples of this prohibition include employees using a government computer and Internet

connection to run a travel business or investment service. The ban on using government-provided IT to support a personal private business also includes employees using that technology to assist relatives, friends, or other persons in such activities.

8.6 The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.

8.7 The creation, download, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.

8.8 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 and sale of goods or services).

8.9 Engaging in any outside fund-raising activity; endorsing any organization, product, or service; participating in any lobbying activity; or engaging in any prohibited political activity.

8.10 Use for posting agency information to external newsgroups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate Agency approval has been obtained.

8.11 Any *other* use that ~~could~~ generate*s* ~~more than minimal~~ *significant* additional expense to the government.

8.12 The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

8.13 Any personal use that could negatively affect the security of the network, including downloading, installing, and/or use of software that is specifically prohibited by DISAI 630-225-13, Software Standards for DISA Network (DISANet) Enterprise Administrative Desktop. ~~, or the DISA Enterprise Software List at https://workspaces.disa.mil/gm/document-1.9.145693~~

8.14 Use of government-provided IT by anyone other than an authorized Federal Government employee. ~~working in their official capacity.~~

9. **No Privacy Expectations**. DISA personnel do not have a right, nor should they have an expectation, of privacy while using any government-provided IT, as detailed in the DoD Chief Information Officer (CIO) Memorandum, Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement, 9 May 2008. (Memorandum is posted at http://dodcio.defense.gov/Portals/0/Documents/DoDBanner-9May2008-ocr.pdf.)

10. **Sanctions for Misuse.** Unauthorized or improper use of government-provided IT could result in immediate revocation of system access and/or user privileges; job counseling and/or admonishment; revocation of security clearance; Uniform Code of Military Justice (UCMJ) and/or criminal prosecution; disciplinary action, reassignment, discharge, or loss of employment; and/or employees being held financially liable for the cost of improper use.

10.1 The provisions of ~~reference 4.1~~ *DoD 5500.7-R (authority document)* concerning the official and authorized use of federal communications constitute lawful general orders or regulations within the meaning of Article 92 (10 United States Code [USC] section 892) of the UCMJ are punitive and apply without further implementation. In addition to prosecution by court-martial under the UCMJ, a violation may serve as a basis for adverse administrative action and other adverse action authorized by the USC or federal regulations. In addition, violation of any provision in ~~reference 4.1~~ *DoD 5500.7-R* may constitute the UCMJ offense of dereliction of duty or other applicable punitive articles.

10.2 Violation of any provision in ~~reference 4.1~~ *DoD 5500.7-R* by DoD civilian employees may result in appropriate criminal prosecution, civil judicial action, disciplinary or adverse administrative action, or other administrative action authorized by USC or federal regulations.

11. **Responsibilities.**

11.1 ***Principal Director for Enterprise Information Services (EIS)/*Chief Information Officer (CIO).** The *Principal Director, EIS /*CIO, will maintain the list of permissible software.

11.2 **Principal Directors, Directors, Commanders, and Chiefs of Major Organizational Elements.** These individuals will ensure personnel comply with authorized unofficial use policies and, if necessary, discipline personnel in accordance with DISAI 220-15-55, Civilian Personnel Management Manual, and U.S. Code, title 10, chapter 47, Uniform Code of Military Justice.

11.3 **Manpower, Personnel, and Security Directorate (MPS) Chief, Security Division (MPS6).** The Chief, MPS6, will ensure investigations are conducted on security violations involving the possible compromise of classified information.

11.4 **Inspector General (IG).** The IG will:

11.4.1 Exercise right of first refusal in investigating network misuse involving pornography.

11.4.2 Coordinate investigations of criminal misuse with the Defense Criminal Investigative Service and, when seizure of computer and/or IT equipment is necessary to an investigation, execute the seizure after consultation with the General Counsel.

11.4.3 Refer matters of misuse deemed to be noncriminal in nature to the user's directorate for appropriate disciplinary and/or administrative action.

12. **Network Manager Duties.** Network managers will:

12.1 Establish and implement appropriate auditing and control processes and procedures to detect misuse and to ensure the efficient and effective use of network resources.

12.2 Ensure all network users have signed user agreements prior to being granted network access in accordance with DISAI 630-230-19, Information Assurance (IA).

12.3 Report instances of access to pornography directly to the IG for determination of investigative requirements.

12.4 Provide the IG with server logs and other forensic documentation, as requested, to support investigations of misuse and, at IG request, lock user accounts.

HENRY.FREDERICK.A
NTHONY.1011175445

FREDERICK A. HENRY
Brigadier General, USA
Chief of Staff

---

*This Instruction replaces DISAI 630-225-15, 14 August 2008, and must be reissued, canceled, or certified current within 5 years of its publication date. If not, it will expire 10 years from its publication date and be removed from the DISA issuances postings.
OPR: ~~CIO~~ *EIS* - disa.meade.eis.mbx.eis-front-office@mail.mil
DISTRIBUTION: ~~Y~~ *P*