
# ADS Chapter 541

# Information Management

Partial Revision Date: 11/14/2014
Responsible Office: M/CIO/CE
File Name: 541_111414

**Functional Series 500: Management Services**
**ADS Chapter 541 - Information Management**
**POC for ADS 541: TBD**

## Table of Contents





*Text highlighted in yellow indicates that the adjacent material is new or substantively revised.*

**Functional Series 500: Management Services**
**ADS Chapter 541 - Information Management**

## 541.1 OVERVIEW

Effective Date: 08/30/1999

This chapter provides the Agency's mandatory policies and required procedures regarding the use of U.S. Government (USG) office equipment and related information technology (IT) resources. This chapter also provides the overall framework for information management at USAID, which is designed to support its mission, goals, and objectives.

The personal use policy establishes privileges and additional responsibilities for USAID employees consistent with authorities affecting employees in the Executive Branch of the Federal Government regarding the use of these resources. It recognizes employees as responsible individuals who are the key to making Government more responsive to its citizens. It allows employees to use Government office equipment for non-Government purposes when such use involves minimal additional expense to the Government, is performed on the employee's non-work time, does not interfere with the mission or operations of a department or agency, or require the installation of software or hardware components that are not Agency standard or Y2K (year 2000) compliant, and does not violate the **Standards of Ethical Conduct for Employees of the Executive Branch**.

Specific governing provisions on use of equipment and services, inappropriate personal use of such resources, proper representation, access management, privacy expectations, and sanctions for misuse are addressed in section **541.3.2**.

## 541.2 PRIMARY RESPONSIBILITIES

Effective Date: 12/15/2010

**a. The Chief Information Officer (CIO)** has overall responsibility and authority for approving the Agency-wide information technology budget. The CIO also has overall responsibility for planning and budgeting activities for information technology-related investments that benefit USAID. The CIO is designated by the Administrator with the approval of the Office of Management and Budget (OMB). (See **Executive Order 13011**)

**b. The Deputy Chief Information Officer (D/CIO)** is responsible for assisting the CIO in meeting all management requirements of the **Clinger-Cohen Act of 1996**, **OMB Circular A-130**, and other related statutes and regulations, including the planning and budgeting components of those statutes and regulations. The Deputy CIO is designated by the CIO.

**c. Heads of Agency Bureaus/Independent Offices/overseas organizations** are responsible for the information content of Agency corporate information systems, consistent with the policies, standards, and guidelines for such systems as established by the Deputy CIO.

Agency organization heads are delegated authority, as appropriate, by the Chief Information Officer (CIO) and Deputy CIO to undertake certain information management functions (see **5 USC Sec. 301**). They are responsible for developing, maintaining, and ensuring the quality of the content of corporate information systems in their areas of program responsibility; for ensuring that data and records contained in information systems are periodically evaluated; and, as needed, improved for accuracy, completeness, and reliability.

Additionally, they are responsible for reporting to M/CIO all corporate information systems (both automated and manual) that are developed, maintained, and operated by each organization.

**d. Supervisory Managers** are responsible for the appropriate use of information management (IM) resources for official Agency business, and for upholding the mandatory policies and procedures governing their employees' use of IM resources as cited in this chapter.

## 541.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 08/30/1999

The statements contained within the .3 section of this ADS chapter are the Agency's official information management mandatory policies and required procedures.

### 541.3.1 Information Management

Effective Date: 05/08/1996

Agency information is a corporate resource. Its management extends through the collection, creation, processing, transmission, dissemination, maintenance, archiving, and disposal of the information.

### 541.3.2 Personal Use Of Information Management (IM) Resources

Effective Date: 08/30/1999

In addition to using office equipment information technology resources in performing official duties, employees may be authorized limited personal use of such Government resources as a conditional privilege. This personal use of information technology must not result in loss of employee productivity nor interfere with official duties. (See **Model "Limited Personal Use" Policy of Government Equipment Including Information Technology – U.S. CIO Council (May 19, 1999))** Moreover, such use must incur only minimal additional expense (defined further in any specific Agency directive that

implements this policy) to the Government and is subject to restrictions in areas such as the following:

- Communications infrastructure costs; for example, telephone charges and telecommunications traffic;
- Use of consumables in limited amounts; for example, paper, ink, and toner;
- General wear and tear on equipment;
- Data storage on storage devices;
- Transmission impacts with moderate e-mail message sizes such as e-mails with small attachments.

Supervisors and employees must refer to sections **541.3.2.1** through **541.3.2.5** regarding the appropriate and inappropriate uses of Agency information management technology resources.

### 541.3.2.1 Inappropriate Personal Uses

Effective Date: 08/30/1999

Employees are expected to conduct themselves professionally in the workplace and to refrain from using Government office equipment for inappropriate activities. Employees may, for example, make limited use under this policy of Government office equipment to check their Thrift Savings Plan or other personal investments, or to seek employment, or communicate with a volunteer charity organization. Misuse or inappropriate personal use of Government office equipment includes the following:

- Any use that incurs more than minimal additional expense to the Government.
- Any personal use that may cause congestion, delay, or disruption of service to any Government system or equipment; for example, greeting cards, video, sound, or other large file attachments that can degrade the performance of the entire network. "Push" technology on the Internet, and other continuous data streams that also degrade the performance of the entire network, are considered inappropriate uses.
- Using the Government systems as a staging ground or platform to gain unauthorized access to other systems.
- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.

- Use 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.

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

- 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.

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

- Use for posting Agency information to external newsgroups, bulletin boards, or other public forums without authority. This includes any use at odds with the Agency's mission or positions, or any use that creates the perception that the communication was made in one's official capacity as a Federal Government employee, unless the Agency has granted official approval.

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

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

- Use to assist relatives, friends, or other persons in commercial or "for profit" activities or other outside employment or business activity.

### 541.3.2.2 Proper Representation of Official Position

Effective Date: 08/30/1999

Employees must not give the false impression that they are acting in an official capacity when they are using Government office equipment for non-Government purposes. (See **Section 2635.702(a) of "Standards of Ethical Conduct for Employees of the Executive Branch,"** United States Government, Office of Ethics.) If such personal use could be interpreted to represent the Agency, then the employee must use an adequate

disclaimer. One acceptable disclaimer is, "The contents of this message are mine personally and do not reflect any position of the Government or my agency."

### 541.3.2.3 Access Management

Effective Date: 08/30/1999

Employees have no inherent right to use Government office equipment for personal use. Therefore, the Agency will establish appropriate controls to ensure that the equipment is used appropriately.

### 541.3.2.4 Privacy Expectations

Effective Date: 11/14/2014

USAID employees have neither a right nor may they have an expectation of privacy while using any Government office equipment at any time, including accessing the Internet and using e-mail.

To the extent that employees wish that their private activities remain private, they must avoid using the Agency office equipment such as their computer, the Internet, or e-mail. By using Government office equipment, Executive Branch employees imply their consent to monitoring, recording, or disclosing the contents of any files or information maintained or passed-through Government office equipment. Employees using Government communications resources must understand that such use is generally not secure, is not private, and is not anonymous.

System managers do employ monitoring tools to detect improper use as defined in this chapter. Any electronic communications may be disclosed within the Agency to officials who have a need to know in the performance of their duties; for instance, when the Chief Information Officer (CISO), Office of Security, or General Counsel needs to gain access to an employee's e-mail accounts or phone calls and records for the investigation of a case. Further,

(1) Per the authorities contained within the IG Act of 1978, the Office of the Inspector General (OIG) may request in writing from the CISO electronic records in the course of investigative matters.

(2) The Director of the Office of Security (SEC) has delegated authority from the Director of National Intelligence (Security Executive) and the Office of Personnel Management (Suitability Executive) to conduct a range of investigations of direct hire and contract employees related to personnel actions, physical or logical facilities access, counterintelligence issues and concerns as well as the insider threat program. Specific authorities related to these activities are referenced in ADS 101. In the performance of these duties, the Director of the Office of Security (SEC) may request in writing from the CISO electronic records in the course of investigative matters.

(3) The Assistant General Counsel for Ethics and Administration (GC/EA) is tasked with assuring that Agency administrative inquiries are conducted consistently and appropriately. Therefore, all personnel related administrative inquiries), under any authority, must be coordinated with and cleared by GC/EA. To the extent that forensic searches by CISO are deemed necessary pursuant to any administrative inquiry, the specific parameters of such a search must be cleared in advance by GC/EA. Forensic searches in relation to an administrative inquiry must be based on a specific need, must be tailored to the circumstances of the allegation, and must be conducted with the minimum intrusion. Under no circumstances may a forensic search be authorized to locate communications that are protected under the Whistleblower Protection Act or any other protected activity.

(4) The Assistant General Counsel for Litigation and Enforcement may request in writing from the CISO electronic records in order to carry out the office's functions.

### 541.3.2.5 Sanctions for Misuse

Effective Date: 08/30/1999

USAID may restrict or revoke an employee's use of information equipment and apply disciplinary or adverse action criminal penalties in the event the employee has misused the equipment or otherwise used it without authorization. Additionally, USAID may hold employees financially liable for the cost of improper use.

## 541.4 MANDATORY RERERENCES

### 541.4.1 External Mandatory References

Effective: 08/30/1999

**a.** **5 USC Sec. 301**

**b.** **Clinger-Cohen Act of 1996**

**c.** **Executive Order 13011**

**d.** **Office of Management and Budget Circular A-130**

**e.** **The Paperwork Reduction Act of 1995**

**f.** **USG Office of Ethics, "Standards of Ethical Conduct for Employees of the Executive Branch," sec. 2635.702(a)**

### 541.4.2 Internal Mandatory References

Effective Date: 08/30/1999

**a.** **Model "Limited Personal Use" Policy of Government Equipment Including Information Technology – U.S. CIO Council (May 19, 1999)**

## 541.5 ADDITIONAL HELP
Effective Date: 12/15/2010

There are no Additional Help documents for this chapter.

## 541.6 DEFINITIONS
Effective: 12/15/2010

The terms and definitions listed below have been included into the ADS Glossary. See the **ADS Glossary** for all ADS terms and definitions.

**Agency organizations**
In USAID/Washington (USAID/W) this includes Bureaus and Independent Offices. Overseas this includes USAID Missions, USAID Offices, USAID Sections of Embassy, Offices for Multi-country Programs, Offices for Multi-country Services, etc. ADS Major Functional Series 100 (Chapters 541, **542**, **543**)

**employee non-work time**
Employee non-work time means times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use Government office equipment during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times). (Chapter 541)

**Government office equipment**
Government office equipment and information technology includes, but is not limited to: personal computers and related peripheral equipment and software, library resources, telephones, facsimile machines, photocopiers, office supplies, Internet connectivity and access to internet services, and e-mail. This list is provided to show examples of office equipment as envisioned by this policy. Executive Branch managers may include additional types of office equipment. (Chapters **518**, 541)

**information management**
The planning, control, and operations of the resources, methodology, and tools required to properly capture, store, and deliver information to Agency employees in a timely, accurate, and economical manner. (Chapter 541)

**information technology (IT)**
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission of reception of data or information by the executive agency. For purposes of the preceding sentence, equipment within an executive agency is associated with corporate or business operations which (i) requires the use of such equipment or (ii), requires the use to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

- The term ‘information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

- The term `information technology' does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (Source: Clinger-Cohen Act) (Chapters **518, 541-548, 552, 577**)

**minimal additional expense**
Minimal additional expense means that employee's personal use of Government office equipment is limited to those situations where the Government is already providing equipment or services and the employee's use of such equipment or services will not result in any 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, making occasional brief personal phone calls (within Agency policy and 41 CFR 101-35.201), infrequently sending personal e-mail messages, or limited use of the Internet for personal reasons. (Chapter 541)

**personal use**
Personal use means activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. Executive Branch employees are specifically prohibited from using Government office equipment 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. (Chapter 541)

**privilege**
Privilege means, in the context of ADS 541, that the Executive Branch of the Federal Government is extending the opportunity to its employees to use Government property for personal use in an effort to create a more supportive work environment. However, this policy does not create right to use Government office equipment for non-Government purposes. Nor does the privilege extend to modifying such equipment, including loading personal software, or making configuration changes. (Chapter 541)

541_111414