Functional Series 400 **INTERIM UPDATE 06-07**
Personnel

SUBJECT: Integration of Telework in Agency Continuity of Operations Plan

NEW MATERIAL: The Agency is issuing this Notice to provide policy guidance on the use of telework in emergency situations. Recent guidance issued by the U.S. Office of Personnel Management (OPM) on emergency planning has emphasized the role of telework.

EFFECTIVE DATE: 08/16/2006

ATTACHMENT: Telework Agreement

POLICY

USAID General Notice
M/HR/PPIM
08/16/2006

SUBJECT: Integration of Telework in Agency Continuity of Operations Plan

The Agency is issuing this Notice to provide policy guidance on the use of telework in emergency situations. Recent guidance issued by the U.S. Office of Personnel Management (OPM) on emergency planning has emphasized the role of telework. (For additional information, see OPM's web pages, located at: http://www.opm.gov/emergency and http://www.opm.gov/pandemic.)

This guidance is primarily intended for USAID/Washington Headquarters but Mission management should review it closely for use in overseas contingency planning, as appropriate.

1. Background

The ability of the Agency to ensure continuity of essential business operations has been and will continue to be very important in times of emergency situations. Increased threats of terrorism, possible pandemic influenza outbreak, and workplace violence have required the Agency to re-evaluate its emergency preparations and to consider other options, such as telework, as an essential part of its continuity of operations planning. Through the use of alternative worksites, Federal employees who were

displaced because of the terrorist attacks on September 11, 2001, and subsequent anthrax attacks were able to continue critical work functions.

The Agency must have the ability to continue essential operations during a wide range of potential emergencies if any portion of the Ronald Reagan Building and other USAID facilities within the Washington, D.C., area become non-operational. In recent years, there have been occasions for using telework arrangements when there have been demonstrations or other events that have caused major disruptions in the Washington, D.C. area.

2. What is Telework and how does it relate to Continuity of Operations Plan (COOP)?

Telework, also referred to as telecommuting, flexiplace, and flexiwork, is an alternative work arrangement in which employees conduct some of their work away from the primary work site.

USAID has incorporated telework in its continuity of operations planning to establish a teleCOOP work arrangement during COOP activation or for other emergency closure situations. Telework is not intended to be a substitute for COOP, but rather is a tool that can be used to augment a COOP activation and to provide alternatives for different emergency situations.

Use of teleCOOP work arrangements will ensure the Agency has the ability to continue critical work operations during a wide range of potential emergencies if any portion of the RRB and other USAID facilities within the Washington, D.C., area become non-operational.

3. Application to Key Staff who Perform Critical Functions

USAID has identified Agency and Bureau/Independent Office (B/IO) critical functions and key staff members to perform essential functions at the Emergency Relocation Site (ERS), at home, or alternate worksites during COOP activation or other emergency closure situations that prohibit occupancy in the Ronald Reagan Building and other USAID facilities for an extended period.

Under the COOP, key staff members in each B/IO have been designated to serve as COOP Coordinator or to serve on one of three teams: the Critical Response Team (CRT), the Critical Function Team (CFT), and the Critical Operations Staff (COS).

COOP Team Members and COOP Coordinators must be prepared and in a state of readiness to promptly report to the Agency's ERS, home worksite, or another alternative worksite, should the COOP be activated or an Agency emergency closure occurs where employees are prevented from reporting to the RRB.

4. Next Steps

To facilitate the use of telework during COOP activation or other emergency, the Agency directs B/IO management to take the following actions:

a) All key staff members who have been designated as a COOP Coordinator or to serve on one of the three COOP Teams mentioned above must review and complete the attached TeleCOOP Work Agreement with their immediate supervisor. This agreement outlines in detail the terms, conditions, expectations, and responsibilities related to performing essential functions at alternative worksites, in addition to the Agency's designated Emergency Relocation Site. B/IO management must ensure that the responsible COOP Team Members and COOP Coordinator are placed under a TeleCOOP Work Agreement within ten (10) working days of the date of issuance of this Notice. Upon completion of these agreements, B/IO management must maintain them as part of its supplementary COOP documentation. TeleCoop Work Agreements must be renewed on an annual basis.

b) The USAID computer system can be accessed remotely through the use of Server Based Computing (SBC) tokens. Tokens can be used at any computer terminal with Internet capability to access the Agency's network. All members of the COOP team should already have SBC tokens. B/IO management must ensure that SBC tokens have been issued to all key staff and that any newly designated COOP team members are provided SBC tokens.

c) All COOP Team Members and COOP Coordinators must be familiar with communicating electronically with colleagues and clients without face-to-face contact. They must have experience functioning in a virtual office that is linked via computer and telephone from home.

d) B/IO management must ensure that all telephone trees are kept up-to-date and include home and cell phone numbers of each COOP team member. This information must be updated on a regular basis and provided to team members for them to retain at their home worksite.

e) To maximize the use of telework during emergencies, Agency work should be organized to facilitate electronic communications, and paper-based processes should be eliminated whenever possible.

5. Safeguarding of Government Information

Employees are prohibited under any circumstances from taking any classified documents from the official worksite to an alternative worksite. In addition, electronic data files with Sensitive But Unclassified (SBU) information that contains Personally Identifiable information must not be let outside of the network.

During a period of activated COOP status or other emergency closure, the removal and use of: 1) Sensitive But Unclassified (SBU) information, 2) Privacy Act and other personal information, and 3) For Official Use Only information at the alternative worksite must be approved by the employee's supervisor. This information must be transported from the official worksite to the alternative worksite in a secure container (e.g., briefcase with lock).

If an employee is permitted to remove SBU, For Official Use Only, Privacy Act, or other personal information, the employee is responsible and accountable for controlling and safeguarding this information. This information may be accessed from employee-owned equipment but must not be stored there. When such information is displayed on a computer screen, it must not be visible to others. The employee is responsible for ensuring that others cannot view the computer screen. Otherwise, employees must use a computer privacy screen which blocks PC screen visibility. Information in hard copy must be kept in a secure file cabinet at the alternative worksite.

Employees must take appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records containing personally identifiable information and to protect against any anticipated threats or hazards to their security or integrity.

As recently demonstrated, the loss or misuse of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Failure to safeguard personally identifiable information can result in disciplinary action, up to and including termination.

For additional information on the handling and safeguarding of Government information: see ADS 508, Privacy Act - 1974, ADS 545, Information Systems Security, ADS 568, National Security Information and Counterintelligence Security Program, and the Executive Message dated 6/8/2006, "Penalties for Violating the Privacy Act of 1974."

6. On-Line Telework Training for Managers and Employees

All managers and employees, especially those who are serving as COOP Team Members and COOP Coordinators in their respective B/IOs, are strongly encouraged to take the on-line telework training courses available on www.telework.gov. There are two courses: Telework 101 for Employees and Telework 101 for Managers.

7. Additional Information and Resources

This Notice will be incorporated as an internal mandatory reference to ADS 405, Telecommuting. It will be posted on the Office of Human Resources (M/HR) Work/Life Webpage located at: http://inside.usaid.gov/M/HR/tele.html, and the Office of Administrative Services, Facilities Management Division (M/AS/FMD) webpage located at: http://inside.usaid.gov/M/AS/FMD/coop.html.

For questions concerning the Agency COOP, please contact Peter Garcia, M/AS/FMD, on (202) 712-1869.

For questions regarding the handling and safeguarding of information, please contact Phil Heneghan, Acting Chief Information Officer (M/CIO), on (202) 712-4938.

For questions regarding telework, please contact Joann Jones, M/HR/PPIM, on (202) 712-5048.

POINT OF CONTACT: Joann Jones, M/HR/PPIM, on (202) 712-5048.

Attachment: USAID TeleCOOP Work Agreement

Notice 0839

File Name	Notice Date	Effective Date	Editorial Revision Date	ADS CD No.	Remarks
IU4_0607_081706_cd45.doc	08/16/2006	08/16/2006		ADS CD 45	This IU will remain active until the policies and procedures in it are incorporated into the ADS as a mandatory internal reference to ADS 405.

Iu4_0607_081706_w081806_cd45