



Guidance for Additional Work-Related Costs Incurred as a Result of Mandated Telework

A Mandatory Reference for ADS Chapter 405

New Edition Date: 05/15/2020
Responsible Office: HCTM
File Name: 405maa_051520

This document supplements [ADS 405, Telework](#) by providing guidance on using Agency funds to offset certain added telework expenses that are directly related to an employee performing telework in response to COVID-19. The objective of this guidance is to continue the Agency's critical foreign policy and national security functions. This guidance applies to all USAID staff, including Direct-Hire employees, Personal Service Contractors, and fellows or individuals under inter-agency service or program agreements (Participating Agency Service Agreement/Participating Agency Program Agreement) working in the U.S. and overseas, but does not apply to institutional support contractor staff. Differences in guidance are noted by specific hiring type or contract mechanism below.

For employees assigned outside of the U.S., telework continues to fall under the authority of their Chief of Mission. If an employee is faced with incurring additional information technology (IT)-related costs to support the Agency's mission by working from an approved alternative worksite (e.g., purchasing a computer or internet service), USAID may grant special allowance payments, based on a case-by-case analysis, to offset certain added expenses that are directly related to performing work from an alternative worksite during a pandemic health crisis (see [5 CFR 550.409\(b\)](#) and [ADS 610](#) (section 610.3.7, Necessary Expense Doctrine)).

If an employee requires USAID to provide or make work-related changes due to a medical condition, refer to [ADS 111, Procedures for Providing Reasonable Accommodation for Individuals with Disabilities](#) for guidance on requesting reasonable accommodation.

1. Agency Funds for Telework-Related Costs

- [ADS 601, Funding Source Policy](#) for guidance on the appropriate use of program or Operating Expense (OE) funding.
- [COVID-19 Task Force Updates: Requesting Operating Expense \(OE\) Funding for COVID-19 Related Activities.](#)

2. Identifying Added IT Expenses Incurred as a Result of Telework in Response to COVID-19

- 2.1** For employees who are unable to perform their official duties by teleworking during the pandemic due to inadequate IT equipment or internet connectivity, the Agency established a process to request necessary IT equipment and/or services (e.g., internet connectivity) to facilitate telework.
- 2.2** In considering such requests, it is the Agency's policy to provide the employee with government-furnished equipment (GFE) as a first option to meet an employee's IT needs for telework, including Agency laptops and/or equipment that may also serve as a Wifi hotspot to provide internet connectivity.

- a. When the Bureau for Management, Office of the Chief Information Officer (M/CIO) determines that providing the employee with GFE is not an effective solution, the employee must work with their supervisor and/or the Mission's Executive Officer (EXO) to identify additional IT equipment and/or services needed to carry out the employee's key responsibilities while teleworking, as well as related and reasonable costs.
 - b. Alternatives, such as the local purchase of IT equipment, the use of the employee's personal device to facilitate connectivity, and/or using Agency funds to pay for an employee's personal internet service for official use, are considered as a last option when M/CIO determines that providing GFE to the employee is not feasible.
- 2.3** The employee must provide their request for IT equipment and/or services to facilitate teleworking to their supervisor for approval. The supervisor determines whether the request is appropriate and reasonable. When approved, the supervisor works with the Bureau/Independent Office's (B/IO) Administrative Management Services (AMS) Officer or the Mission's EXO to prepare the [Mandatory Telework Mission IT Request Questionnaire](#) for M/CIO's review and approval. The AMS Officer or EXO submits the employee's request to M/CIO, who reviews and approves the suitability of the requested IT equipment and/or services within the Agency's IT environment.
- 2.4** Use of Agency funds to pay for the employee's added telework expenses during the pandemic may be in the form of:
- a. Agency payment to a vendor for the purchase of IT equipment.
 - b. Agency payment to the employee to reimburse the employee's documented payment of internet services (e.g., monthly internet connection), provided that the service was necessary for the employee to telework (see **sections 3** and **4** of this document for additional considerations when reimbursing employees).

3. Evaluating the Employee's Request for Reimbursement of Personal IT Service

- 3.1** The Agency may consider reimbursing a portion of an employee's payment of the billing period's charges for the employee's personal internet connectivity.
- a. Domestic employees: Providing GFE is expected to address the domestic employee's need for internet connectivity (see **section 2.2**). Employees assigned to/working in the United States requesting reimbursement of IT services will be handled on a case-by-case basis.
 - b. Overseas employees: Providing GFE may not be feasible to meet an overseas employee's need for increased internet connectivity (e.g.,

inability to ship GFE to overseas employees). M/CIO will make this determination and, in some cases, will then consider alternatives such as reimbursement.

3.2 The employee must disclose any personal benefits provided by the internet service provider (e.g., free equipment or other promotional items or rebates, bundled services, discounts). When determining the amount to be reimbursed by the Agency, the value of these personal benefits must be discounted from the internet service provider's costs.

3.3 As stewards of federal funds, reimbursement requests must include the following assurances:

a. The employee must provide written certification that the requested reimbursement amount is directly and exclusively attributed to the conduct of official USAID business and excludes or prorates all personal use of the internet service, and that the business use complies with the Agency policies, including the Rules of Behavior outlined in [ADS 545mbd](#). The employee's certification is required for each billing period, when reimbursement is being requested.

b. Designated official(s) approving the employee's request must:

- Confirm that the requested amount for reimbursement is directly and exclusively attributed to time spent conducting official USAID business during that month. Example activities include, but are not limited to: obtaining the employee's certification noted in **section 3.3.a**, comparing the employee's hours worked against the percentage of internet costs being reimbursed, obtaining disclosures from the employee of any personal benefits provided by the internet service provider, etc.
- Ensure that adequate controls are in place to prevent improper reimbursement for the employee's personal use of internet services. Example activities include, but are not limited to: monitoring the employee's performance and productivity on a bi-weekly and monthly basis, periodically reviewing payments to identify trends, etc. (see [ADS 596, Management's Responsibility for Internal Control](#), for additional guidance on controls).

4. Approving the Employee's Request for Reimbursement of IT Services

4.1 The authority to approve the employee's requested reimbursement amount is dependent on the supervisor's approval. If the employee's requested reimbursement amount exceeds \$100 per month, then the approval of the employee's B/IO Head or Mission Director is required.

4.2 The B/IO or Mission has discretion to determine whether the employee's request for reimbursement is appropriate (e.g., business need and dollar amount). Required documentation to support this determination include:

- a. Copy of the invoice from the employee's internet service provider, and a certification from the employee on what portion relates to usage for official USAID purposes (see **section 3.3**).
- b. The controls in place to prevent reimbursement for the employee's personal use (see **section 3.3**).

4.3 Missions should consider and address the impact of local laws on approving such reimbursements, as well as any host country government limitations on access and usage.

5. Safeguarding the Integrity of Federal Funds Used for Reimbursement

5.1 USAID policies and procedures concerning employee roles and responsibilities in the workplace continue to be applicable in the telework environment (e.g., Rules of Behavior ([ADS 545mbd](#)), code of conduct, ethics, protecting government data and physical assets, fiscal integrity, performance, conduct, prohibitions and restrictions on accessing classified information, etc.). These policies and procedures will apply for the duration of the time that the employee is performing official duties, even if the employee is using personal internet to perform official business.

5.2 All employees are prohibited from reading, discussing, or storing classified materials in unrestricted spaces at any time (see [ADS 568, National Security Information Program](#)).

5.3 Documentation supporting the reimbursement of the employee's internet costs from an alternate worksite, and the employee's use of internet services, must adhere to existing USAID policies and procedures, including but not limited to:

- [ADS 502, The USAID Records Management Program](#),
- [ADS 545, Information Systems Security](#), and
- [ADS 620, Financial Management Principles and Standards](#).

5.4 USAID may periodically review a B/IO or Mission's reimbursement process to ensure adequate safeguard against private misuse and to ensure payments are proper and in place (e.g., directly attributed to the employee's use of personal internet services for official USAID purposes) (see [ADS 630, Payables Management](#)).