Save the Children provides the following comments in response to the proposed changes to the USAID Partner Information Form (PIF). The comments pertain to seven fields of the proposed PIF, fields 4a.16 through 4a.22. We can provide additional information in writing or via a phone call, if that would be helpful.

- Changing three fields ("4a.16 Address of Residence," "4a.17 Province/Region," and "4a.18 Tribal Affiliation *(if applicable)*") from *optional* to *mandatory* is not necessary for the proper functions of USAID. USAID has already complied with its requirements under ADS Chapter 319 with these fields as *optional* (see PIF expired 12/31/2022). Switching these fields to *mandatory* at this point is not necessary to ensure compliance with ADS Chapter 319.
- Replacing four fields ("Primary Phone Number," "Alternate Phone Number," "Primary Email Address," and "Alternate Email Address") ("Group A") with four updated fields (""4a.19 Primary Personal Phone Number *(Include full phone numbers, country code, and area/city code)*," "4a.20 Alternate Personal Phone Number *(if applicable) (Include full phone number, country code, and area/city code)*," "4a.21 Primary Personal Email Address," and, "4a.11 Alternate Personal Email Address *(if applicable)"* ("Group B") is not necessary for the proper functions of USAID. USAID has already complied with its requirements under ADS Chapter 319 via its use of the Group A fields (see PIF expired 12/31/2022). Replacing Group A fields with Group B fields at this point is not necessary to ensure compliance with ADS Chapter 319.
- The estimated time burden for respondents is likely inaccurate. The estimated time burden for both PIF versions in 90 minutes, but the collection of data for 4a.16 through 4a.22 will arguably take much longer to complete. The request for 4a.16 through 4a.22 will almost certainly be met with resistance by staff, trustees, and others reluctant to provide personal information such as their home address, personal cell phone number, and personal email address. Prime recipients will need to spend a greater percentage of their time explaining to individuals why their personal data is needed and convincing them to provide it. There may even be situations in which individuals refuse to provide their address, personal phone number, and personal email address, resulting in significant delays with program implementation and possible termination for failure to comply.
- There is no obvious utility of the personal data in 4a.16 through 4a.22. These data points are unrelated to an individual's relationship with their employers or the activities they are involved with.
- Primes and subs subject to UK law are prohibited from disclosing personal data they control to third parties where the third party hasn't identified their need for the data. Primes and subs subject to UK law would need more information to understand why USAID requires, for example, the residential addresses of staff members and trustees, as well as their personal phone numbers, email addresses, and tribal affiliations. US security is too broad to enable organizations to meet the regulatory requirement under UK law of establishing the necessity for the requested data. If a need for the personal data can be presented in appropriate detail, this would be a helpful first step. However, UK law also requires organizations to subject the need identified to the legal tests of 'legitimacy' and 'proportionality'. Where data is to be sent to a third

country, as it will with USAID partner vetting, these legal tests are particularly stringent and complicated because (a) the data will be subject to lower legal protections and (b) we have to establish that providing the data serves not just the third country's interest, but a third country's interest recognized in law by the UK. We can likely establish this for the US in relation to the prevention of terrorist financing, however the information requested goes beyond what is required for checking identities against sanctions and terrorist lists.

Primes and subs subject to UK law are also prohibited from sharing the personal data on the basis of consent of the individuals involved. Under UK law, consent only works as a lawful basis to share personal data where it is freely given (the data subject must have a genuine choice). Employees would not be seen as having a genuine choice; therefore, we would need to satisfy the legal hurdles and tests described above.