COUNCIL OF INTERNATIONAL DEVELOPMENT COMPANIES
An initiative of: PSC PROFESSIONAL SERVICES COUNCIL

May 20, 2019
Ms. Carol Kendrick
Bureau of Management
Office of Acquisition and Assistance, Policy Division
SA-44; Room 867-F
Washington, D.C. 20523-2052

Dear Ms. Kendrick:

Recent cyberattacks have been directed at multinational corporations, American cities, individuals, and almost all the agencies of the U.S. government. Perpetrators include malicious individuals, criminal organizations and malevolent nation-states. There is no indication that these attacks will lessen in frequency or damage. As such, PSC has long been a champion of appropriate and vigorous cyber-defense for our member companies and the federal agencies they serve. Therefore, PSC and our Council of International Development Companies appreciate the opportunity to provide the attached feedback to the proposed rule published in the *Federal Register* on March 21, 2019 regarding the U.S. Agency for International Development Acquisition Regulation (AIDAR): Security and Information Technology Requirements.

We are concerned that much of the proposed regulation lacks the clarity, definitional specificity and recognition of potential unintended consequences – particularly as they relate to timely programmatic implementation. The definition, or lack thereof, regarding "Information Technology" will likely result in much confusion and delay. PSC members have already reported to us a year-long delay in the roll-out of a website due to inconsistent interpretations of existing regulations. Similarly, it is quite normal for project delays to occur as some Contracting Officers contend they are required to approve the purchase of every piece of IT hardware – from laptops to thumb-drives. Others require retroactive approvals, while others require none at all. This lack of transparency and consistency is the root of our concerns and the genesis of much of our commentary.

We look forward to addressing any issues that warrant further explanations. If you have any further questions, or need any additional information, please do not hesitate to contact Paul Foldi, PSC's VP for International Development Affairs, or me at (703) 875-8059.

Sincerely,

Alan Chvotkin
EVP & Counsel

Attachment

Professional Services Council
Comments On
U.S. Agency for International Development Acquisition Regulation (AIDAR):
Security and Information Technology Requirements
May 20, 2019

SUMMARY

PSC believes significant clarifying clauses and definitions are warranted throughout the proposed rule. These will avoid confusion and major unintended consequences – some of which our members already report – that cause unwarranted delays, obfuscations, significant hinderances to programmatic implementation, and inconsistent contract administration.

DEFINITIONS

We recommend that the final rule state that the rule will apply to acquisition of IT resources used on the USAID infrastructure only and not on IT *systems* and *services* for implementer operations, development work or for third parties (e.g. host government), nor the US government. The proposed 739.002 does not differentiate between these applications.

In addition, the proposed rule needs to clarify better the definition of "Agency information systems/facilities." As currently drafted, the definition of information technology used in the proposed rule includes:

> "any service, equipment or system or subsystem that are used by the agency….. Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency…. including imaging peripherals, input, output, and storage devices necessary for security and surveillance."

It should instead be defined as Agency IT infrastructure. There are many agency databases developed for USAID that are not connected to the agency IT infrastructure. Similarly, PSC believes a section should be added detailing what/if

any contractor hardware will be impacted by the rule. PSC has already received numerous examples of our members having to petition the agency for permission for laptops and other commercially available, off-the-shelf items purchases. Currently, some COs require prior approval to buy a thumb-drive or cell phone. It is vital for any covered regulations to state if and/or when contractors are required to seek permission to purchase said items. PSC is concerned the USAID person-hours needed to review the purchase of every laptop, thumb-drive, or video conference camera covered by this language would forestall by days, weeks or even months project activity – particularly given the often remote areas in which our members are contracting with the Agency to carry out work.

Additionally, the rule needs to distinguish between IT systems and services for the agency enterprise architecture and contractor operations as opposed to the development implementation and those done for third parties. This includes the need to clarify the "total cost of ownership" role of the CIO. The proposed rule implies that the USAID CIO will assume a role to accomplish project evaluation and technical merits of the projects in more than 100 countries.

We believe clarification is required as to what is the agency's enterprise architecture and what software or application necessitates an alignment with the infrastructure. Similarly, clarification is needed as to the circumstances when the Agency will consolidate licenses in Washington and globally.

CONFLICTING GUIDANCE

Upon finalizing this proposed rule, AAPD 16-02 should be rescinded. We recommend that any matters now included in AAPD 16-02 that are *not* included in the final rule should be included in a *new* AAPD, if necessary.

We understand that ADS 548 has been "sunset" (suspended) and is being rewritten. However, many USAID contracting officers seem unaware of this. We recommend all requirements of ADS 548 be included in the new rule and ADS 548 be marked as "reserved" unless and until a revised and updated version is approved.

We recommend that all USAID policies and procedures be consolidated in the rule instead of using various other USAID guidance mechanisms such as ADS, AAPDs and PEBs.

The rule should harmonize requirements for those *contractors* with PSC, TCN and FSN staff having access to the USAID facilities or information systems vs those USAID personal services contractors (PSC, TCN and FSN) hired directly to do the same work.

USAID-FINANCED THIRD-PARTY WEBSITES

The rule needs to distinguish between web sites that are informational, collect information or include apps, from those connected to USAID infrastructure, facilities or information systems. PSC recommends the rule clarify what the "certain requirements" are when developing, launching and maintaining a third-party website. If a statute, regulation or Executive Order limits collection of information, we recommend that the rule just refer to those statutes, regulations or Executive Orders. Clarification should also be provided regarding what websites are considered to "achieve project implementation goals" and any approval process should be streamlined via one single contact and one single form. PSC members report that USAID Missions often elect not to develop websites due to a complex, unclear and protracted review and approval process.

The rule has many requirements regarding USAID-financed third-party websites. PSC notes it does not discuss third-party websites created under subcontracts under *assistance*. Clarification is needed as to the terms "external to USAID boundaries" and "not directly controlled polices and staff."

The proposed rule requires notification by the contractor to the COR to be provided to the agency's Bureau for Legislative and Public Affairs (LPA) prior for evaluation and approval of website development. PSC notes the rule does not specify what is the evaluation criteria for the approval process of LPA, let alone LPA's personnel or legal capacity to evaluate and approve websites and privacy policy in a timely manner.

The proposed rule requires periodic vulnerability scans. PSC recommends clarification of the definition of "remediation actions" required by the contractor if

vulnerabilities are discovered. If a contractor authorizes the USAID CISO to conduct periodic vulnerability scans via its Web-scanning program, what are the issues and protections of liability for this action?

ROLE OF THE CIO

Regarding Information Technology Approval, clarification is needed to be consistent with FITARA as to "use by the Agency." As written, the rule would apply to all agency IT investment decisions in all contracts. A more complete clarification is needed regarding what defines the agency's enterprise architecture. As written, the Agency CIO would have to analyze every project for ownership, risk, security, privacy and security of the system. See 752.239-xx(b).

SOFTWARE LICENSES

The language regarding terms of service/and conditions, especially as it relates to a "private party" will generate confusion. Who is a "private party"? The text overtly implies that when the federal government buys commercial software it is not going to comply with the commercial license agreements.

The software licensing clause is not clear and can be interpreted to be applicable to implementing partners buying software for project use or for beneficiaries. Clarification is needed as to when this is applicable. Approval of software license renewal will be an undue burden for standard software licenses. PSC recommends a list of exempt software that does not need approval, whether initial approval or at renewal of the license that are commercially available (e.g., Microsoft Office, Adobe, etc.). Otherwise, would this apply to the prime contractor or only when USAID is purchasing licenses? Moreover, most prime contractors have corporate agreements for licenses (for cost effectiveness purposes and faster deployment) where standard licenses are allocated to projects. Will these need approval as well? PSC questions if this is would be a value-added approval.

A more concrete definition of "mutual agreement of the parties" in clause (b) of the Addendum is necessary as it pertains to software renewal, including who is authorized to make such agreements? Additionally, PSC notes that software can be renewed monthly or yearly and may go beyond the end of contract as part of the

commercial license. This is an allowable cost and should not require a specific Agency approval.

OTHER COMMENTS

- The Request for Approval Requirements does not address a grantee that subcontracts for IT.
- PSC believes this section under Limitation on Acquisition of Information Technology (and used elsewhere in the rule) is poorly worded and should be deleted to avoid confusion. It now states:

> "(4) The term 'information technology' does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment."

- The Certified Information Systems Security Professional (CISSP) certification process is unclear. What organizations offer this certification? Similarly, what defines "significant information security responsibilities"?
- PSC is concerned that the Homeland Security Presidential Directive-12 (HSPD–12) and Personal Identity Verification (PIV) portion of the rule restricts access to USAID facilities or logical access to USAID's information systems to only US citizens and resident aliens. As drafted it would require almost all institutional contractors to terminate FSNs, CCNs or TCNs performing critical functions, to include acquisition and assistance functions requiring access to USAID facilities and logical access to USAID's information systems (GLASS, Phoenix, FAADS, FPDS, CPARS etc.). Similarly, this portion of the rule does not address how it would apply to USAID's use of personal services contractors who are FSNs, CCNs and TCNs performing the same functions and are not US citizens or resident aliens.
- The rule requires monthly reports to the COR regarding all staff on the project, including any newly hired or separated contract staff – even if no staff changes were made. PSC notes the rule does not specify what the COR will do with the documents. Clarification is required regarding who is the appropriate Enrollment Office personnel (for Washington and Missions). For

non-US personnel (FSN, CCN or PSC), they may not possess a valid U.S. Federal, State Government-issued picture ID so this provision should be revised. Clarification is also needed as to who is the appropriate USAID Security Office (for Washington and Missions). What is the requirement for "documentation of security background investigation"? Also, clarify "physically present" and where is this applicable, for Washington and/or mission awards?

##