

REQUEST FOR PROPOSALS

TECHNICAL ASSISTANCE FOR THE

NATIONAL CYBERSECURITY MASTER PLAN

Submission Deadline: **5:00 PM**

LOCAL (NAIROBI) TIME

NOVEMBER 18, 2011

Submission Place: Bitange Ndemo
Permanent Secretary
Ministry of Information and Communications
Teleposta Towers, Kenyatta Ave./Koinange St.
P.O. Box 30025
Nairobi, Kenya 00100
Phone: +254-20-2251152
Fax: +254-20-315147

SEALED PROPOSALS SHALL BE CLEARLY MARKED AND RECEIVED PRIOR TO THE TIME AND DATE SPECIFIED ABOVE. PROPOSALS RECEIVED AFTER SAID TIME AND DATE WILL NOT BE ACCEPTED OR CONSIDERED.

REQUEST FOR PROPOSALS

SECTION 1:	INTRODUCTION	4
1.1	BACKGROUND SUMMARY	4
1.2	OBJECTIVE	4
1.3	PROPOSALS TO BE SUBMITTED	4
1.4	CONTRACT FUNDED BY USTDA	5
SECTION 2:	INSTRUCTIONS TO OFFERORS	6
2.1	PROJECT TITLE	6
2.2	DEFINITIONS	6
2.3	DEFINITIONAL MISSION REPORT	6
2.4	EXAMINATION OF DOCUMENTS	6
2.5	PROJECT FUNDING SOURCE	7
2.6	RESPONSIBILITY FOR COSTS	7
2.7	TAXES	7
2.8	CONFIDENTIALITY	7
2.9	ECONOMY OF PROPOSALS	7
2.10	OFFEROR CERTIFICATIONS	7
2.11	CONDITIONS REQUIRED FOR PARTICIPATION	7
2.12	LANGUAGE OF PROPOSAL	8
2.13	PROPOSAL SUBMISSION REQUIREMENTS	8
2.14	PACKAGING	8
2.15	AUTHORIZED SIGNATURE	8
2.16	EFFECTIVE PERIOD OF PROPOSAL	9
2.17	EXCEPTIONS	9
2.18	OFFEROR QUALIFICATIONS	9
2.19	RIGHT TO REJECT PROPOSALS	9
2.20	PRIME CONTRACTOR RESPONSIBILITY	9
2.21	AWARD	9
2.22	COMPLETE SERVICES	10
2.23	INVOICING AND PAYMENT	10
SECTION 3:	PROPOSAL FORMAT AND CONTENT	11
3.1	EXECUTIVE SUMMARY	11
3.2	COMPANY INFORMATION	12
3.2.1	COMPANY PROFILE	12
3.2.2	OFFEROR'S AUTHORIZED NEGOTIATOR	12
3.2.3	NEGOTIATION PREREQUISITES	12
3.3	ORGANIZATIONAL STRUCTURE, MANAGEMENT, AND KEY PERSONNEL	15
3.4	TECHNICAL APPROACH AND WORK PLAN	15
3.5	EXPERIENCE AND QUALIFICATIONS	16
SECTION 4:	AWARD CRITERIA	17

ANNEX 1	FEDBIZOPPS ANNOUNCEMENT
ANNEX 2	EXCERPT FROM DEFINITIONAL MISSION REPORT
ANNEX 3	USTDA NATIONALITY REQUIREMENTS
ANNEX 4	USTDA GRANT AGREEMENT, INCLUDING MANDATORY CONTRACT CLAUSES
ANNEX 5	TERMS OF REFERENCE (FROM USTDA GRANT AGREEMENT)
ANNEX 6	COMPANY INFORMATION

Section 1: INTRODUCTION

The U.S. Trade and Development Agency (USTDA) has provided a grant in the amount of US\$580,000 to The Ministry of Information and Communications (the "Grantee") in accordance with a grant agreement dated September 19, 2011 (the "Grant Agreement"). The grant will fund Technical Assistance to aid the Grantee in determining the technical, operational, and business requirements for developing a cohesive approach to secure Kenya's information and communication technology infrastructure. The Grant Agreement is attached at Annex 4 for reference. The Grantee is soliciting technical proposals from qualified U.S. firms to provide expert consulting services to perform the Technical Assistance.

1.1 BACKGROUND SUMMARY

The Government of Kenya (GoK) plans to implement an e-government program, develop shared services, create national data centers, and utilize cloud computing. All of these plans will create additional government services and efficiencies for Kenyan citizens, but also expose them to cybersecurity threats which both the GoK's network and the private networks are currently unable to address. The National Cybersecurity Master Plan will provide the GoK with a national-level plan to defend and secure its digital infrastructure, as well as recommend minimum cybersecurity standards for the country's private networks. The Master Plan will include the development of information security management controls and procedures, cybersecurity systems, and identity and access management systems. Critically, Technical Assistance also includes the development of procurement documents which take into account concepts such as total lifetime cost of ownership, reliability, scalability, quality, interoperability and conformance to international standards.

A background Definitional Mission performed by RG International Technology Consulting, LLC is provided for reference in Annex 2.

1.2 OBJECTIVE

The objective of this Technical Assistance is to aid the Grantee in the development of procurement documents and provide the Grantee with the tools and technical understanding it needs to evaluate cybersecurity technology bids based on interoperability, scalability, and quality. In this respect, the Technical Assistance will be significant in that it will begin a transformation in how the Grantee procures its ICT infrastructure.

The Terms of Reference (TOR) for this Technical Assistance are attached as Annex 5.

1.3 PROPOSALS TO BE SUBMITTED

Technical proposals are solicited from interested and qualified U.S. firms. The administrative and technical requirements as detailed throughout the Request for Proposals (RFP) will apply. Specific proposal format and content requirements are detailed in Section 3.

The amount for the contract has been established by a USTDA grant of US\$580,000. **The USTDA grant of US\$580,000 is a fixed amount. Accordingly, COST will not be a factor in the evaluation and therefore, cost proposals should not be submitted.** Upon detailed evaluation of technical proposals, the Grantee shall select one firm for contract negotiations.

1.4 CONTRACT FUNDED BY USTDA

In accordance with the terms and conditions of the Grant Agreement, USTDA has provided a grant in the amount of US\$580,000 to the Grantee. The funding provided under the Grant Agreement shall be used to fund the costs of the contract between the Grantee and the U.S. firm selected by the Grantee to perform the TOR. The contract must include certain USTDA Mandatory Contract Clauses relating to nationality, taxes, payment, reporting, and other matters. The USTDA nationality requirements and the USTDA Mandatory Contract Clauses are attached at Annexes 3 and 4, respectively, for reference.

Section 2: INSTRUCTIONS TO OFFERORS

2.1 PROJECT TITLE

The project is called National Cybersecurity Master Plan.

2.2 DEFINITIONS

Please note the following definitions of terms as used in this RFP.

The term "Request for Proposals" means this solicitation of a formal technical proposal, including qualifications statement.

The term "Offeror" means the U.S. firm, including any and all subcontractors, which responds to the RFP and submits a formal proposal and which may or may not be successful in being awarded this procurement.

2.3 DEFINITIONAL MISSION REPORT

USTDA sponsored a Definitional Mission to address technical, financial, sociopolitical, environmental and other aspects of the proposed project. A copy of the report is attached at Annex 2 for background information only. Please note that the TOR referenced in the report are included in this RFP as Annex 5.

2.4 EXAMINATION OF DOCUMENTS

Offerors should carefully examine this RFP. It will be assumed that Offerors have done such inspection and that through examinations, inquiries and investigation they have become familiarized with local conditions and the nature of problems to be solved during the execution of the Technical Assistance.

Offerors shall address all items as specified in this RFP. Failure to adhere to this format may disqualify an Offeror from further consideration.

Submission of a proposal shall constitute evidence that the Offeror has made all the above mentioned examinations and investigations, and is free of any uncertainty with respect to conditions which would affect the execution and completion of the Technical Assistance.

2.5 PROJECT FUNDING SOURCE

The Technical Assistance will be funded under a grant from USTDA. The total amount of the grant is not to exceed US\$580,000.

2.6 RESPONSIBILITY FOR COSTS

Offeror shall be fully responsible for all costs incurred in the development and submission of the proposal. Neither USTDA nor the Grantee assumes any obligation as a result of the issuance of this RFP, the preparation or submission of a proposal by an Offeror, the evaluation of proposals, final selection or negotiation of a contract.

2.7 TAXES

Offerors should submit proposals that note that in accordance with the USTDA Mandatory Contract Clauses, USTDA grant funds shall not be used to pay any taxes, tariffs, duties, fees or other levies imposed under laws in effect in the Host Country.

2.8 CONFIDENTIALITY

The Grantee will preserve the confidentiality of any business proprietary or confidential information submitted by the Offeror, which is clearly designated as such by the Offeror, to the extent permitted by the laws of the Host Country.

2.9 ECONOMY OF PROPOSALS

Proposal documents should be prepared simply and economically, providing a comprehensive yet concise description of the Offeror's capabilities to satisfy the requirements of the RFP. Emphasis should be placed on completeness and clarity of content.

2.10 OFFEROR CERTIFICATIONS

The Offeror shall certify (a) that its proposal is genuine and is not made in the interest of, or on behalf of, any undisclosed person, firm, or corporation, and is not submitted in conformity with, and agreement of, any undisclosed group, association, organization, or corporation; (b) that it has not directly or indirectly induced or solicited any other Offeror to put in a false proposal; (c) that it has not solicited or induced any other person, firm, or corporation to refrain from submitting a proposal; and (d) that it has not sought by collusion to obtain for itself any advantage over any other Offeror or over the Grantee or USTDA or any employee thereof.

2.11 CONDITIONS REQUIRED FOR PARTICIPATION

Only U.S. firms are eligible to participate in this tender. However, U.S. firms may utilize subcontractors from the Host Country for up to 20 percent of the amount of the USTDA grant for

specific services from the TOR identified in the subcontract. USTDA's nationality requirements, including definitions, are detailed in Annex 3.

2.12 LANGUAGE OF PROPOSAL

All proposal documents shall be prepared and submitted in English, and only English.

2.13 PROPOSAL SUBMISSION REQUIREMENTS

The **Cover Letter** in the proposal must be addressed to:

Bitange Ndemo
Permanent Secretary
Ministry of Information and Communications
Teleposta Towers, Kenyatta Ave./Koinange St.
P.O. Box 30025
Nairobi, Kenya 00100
Phone: +254-20-2251152
Fax: +254-20-315147

An Original and eight (8) copies of your proposal must be received at the above address no later than 5:00 LOCAL (NAIROBI) TIME, on NOVEMBER 18, 2011.

Proposals may be either sent by mail, overnight courier, or hand-delivered. Whether the proposal is sent by mail, courier or hand-delivered, the Offeror shall be responsible for actual delivery of the proposal to the above address before the deadline. Any proposal received after the deadline will be returned unopened. The Grantee will promptly notify any Offeror if its proposal was received late.

Upon timely receipt, all proposals become the property of the Grantee.

2.14 PACKAGING

The original and each copy of the proposal must be sealed to ensure confidentiality of the information. The proposals should be individually wrapped and sealed, and labeled for content including "original" or "copy number x"; the original and eight (8) copies should be collectively wrapped and sealed, and clearly labeled.

Neither USTDA nor the Grantee will be responsible for premature opening of proposals not properly wrapped, sealed and labeled.

2.15 AUTHORIZED SIGNATURE

The proposal must contain the signature of a duly authorized officer or agent of the Offeror empowered with the right to bind the Offeror.

2.16 EFFECTIVE PERIOD OF PROPOSAL

The proposal shall be binding upon the Offeror for ninety (90) days after the proposal due date, and Offeror may withdraw or modify this proposal at any time prior to the due date upon written request, signed in the same manner and by the same person who signed the original proposal.

2.17 EXCEPTIONS

All Offerors agree by their response to this RFP announcement to abide by the procedures set forth herein. No exceptions shall be permitted.

2.18 OFFEROR QUALIFICATIONS

As provided in Section 3, Offerors shall submit evidence that they have relevant past experience and have previously delivered advisory, Technical Assistance and/or other services similar to those required in the TOR, as applicable.

2.19 RIGHT TO REJECT PROPOSALS

The Grantee reserves the right to reject any and all proposals.

2.20 PRIME CONTRACTOR RESPONSIBILITY

Offerors have the option of subcontracting parts of the services they propose. The Offeror's proposal must include a description of any anticipated subcontracting arrangements, including the name, address, and qualifications of any subcontractors. USTDA nationality provisions apply to the use of subcontractors and are set forth in detail in Annex 3. The successful Offeror shall cause appropriate provisions of its contract, including all of the applicable USTDA Mandatory Contract Clauses, to be inserted in any subcontract funded or partially funded by USTDA grant funds.

2.21 AWARD

The Grantee shall make an award resulting from this RFP to the best qualified Offeror, on the basis of the evaluation factors set forth herein. The Grantee reserves the right to reject any and all proposals received and, in all cases, the Grantee will be the judge as to whether a proposal has or has not satisfactorily met the requirements of this RFP.

2.22 COMPLETE SERVICES

The successful Offeror shall be required to (a) provide local transportation, office space and secretarial support required to perform the TOR if such support is not provided by the Grantee; (b) provide and perform all necessary labor, supervision and services; and (c) in accordance with best technical and business practice, and in accordance with the requirements, stipulations, provisions and conditions of this RFP and the resultant contract, execute and complete the TOR to the satisfaction of the Grantee and USTDA.

2.23 INVOICING AND PAYMENT

Deliverables under the contract shall be delivered on a schedule to be agreed upon in a contract with the Grantee. The Contractor may submit invoices to the designated Grantee Project Director in accordance with a schedule to be negotiated and included in the contract. After the Grantee's approval of each invoice, the Grantee will forward the invoice to USTDA. If all of the requirements of USTDA's Mandatory Contract Clauses are met, USTDA shall make its respective disbursement of the grant funds directly to the U.S. firm in the United States. All payments by USTDA under the Grant Agreement will be made in U.S. currency. Detailed provisions with respect to invoicing and disbursement of grant funds are set forth in the USTDA Mandatory Contract Clauses attached in Annex 4.

Section 3: PROPOSAL FORMAT AND CONTENT

To expedite proposal review and evaluation, and to assure that each proposal receives the same orderly review, all proposals must follow the format described in this section.

Proposal sections and pages shall be appropriately numbered and the proposal shall include a Table of Contents. Offerors are encouraged to submit concise and clear responses to the RFP. Proposals shall contain all elements of information requested without exception. Instructions regarding the required scope and content are given in this section. The Grantee reserves the right to include any part of the selected proposal in the final contract.

The proposal shall consist of a technical proposal only. A cost proposal is NOT required because the amount for the contract has been established by a USTDA grant of US\$580,000, which is a fixed amount.

Offerors shall submit one (1) original and eight (8) copies of the proposal. Proposals received by fax cannot be accepted.

Each proposal must include the following:

- Transmittal Letter,
- Cover/Title Page,
- Table of Contents,
- Executive Summary,
- Company Information,
- Organizational Structure, Management Plan, and Key Personnel,
- Technical Approach and Work Plan, and
- Experience and Qualifications.

Detailed requirements and directions for the preparation of the proposal are presented below.

3.1 EXECUTIVE SUMMARY

An Executive Summary should be prepared describing the major elements of the proposal, including any conclusions, assumptions, and general recommendations the Offeror desires to make. Offerors are requested to make every effort to limit the length of the Executive Summary to no more than five (5) pages.

3.2 COMPANY INFORMATION

For convenience, the information required in this Section 3.2 may be submitted in the form attached in Annex 6 hereto.

3.2.1 Company Profile

Provide the information listed below relative to the Offeror's firm. If the Offeror is proposing to subcontract some of the proposed work to another firm(s), the information requested in sections 3.2.5 and 3.2.6 below must be provided for each subcontractor.

1. Name of firm and business address (street address only), including telephone and fax numbers.
2. Year established (include predecessor companies and year(s) established, if appropriate).
3. Type of ownership (e.g. public, private or closely held).
4. If private or closely held company, provide list of shareholders and the percentage of their ownership.
5. List of directors and principal officers (President, Chief Executive Officer, Vice-President(s), Secretary and Treasurer; provide full names including first, middle and last). Please place an asterisk (*) next to the names of those principal officers who will be involved in the Technical Assistance.
6. If Offeror is a subsidiary, indicate if Offeror is a wholly-owned or partially-owned subsidiary. Provide the information requested in items 1 through 5 above for the Offeror's parent(s).
7. Project Manager's name, address, telephone number, e-mail address and fax number.

3.2.2 Offeror's Authorized Negotiator

Provide name, title, address, telephone number, e-mail address and fax number of the Offeror's authorized negotiator. The person cited shall be empowered to make binding commitments for the Offeror and its subcontractors, if any.

3.2.3 Negotiation Prerequisites

1. Discuss any current or anticipated commitments which may impact the ability of the Offeror or its subcontractors to complete the Technical Assistance as proposed and reflect such impact within the project schedule.
2. Identify any specific information which is needed from the Grantee before commencing contract negotiations.

3.2.4 Offeror's Representations

If any of the following representations cannot be made, or if there are exceptions, the Offeror must provide an explanation.

1. Offeror is a corporation [*insert applicable type of entity if not a corporation*] duly organized, validly existing and in good standing under the laws of the State of _____. The Offeror has all the requisite corporate power and authority to conduct its business as presently conducted, to submit this proposal, and if selected, to execute and deliver a contract to the Grantee for the performance of the Technical Assistance. The Offeror is not debarred, suspended, or to the best of its knowledge or belief, proposed for debarment, or ineligible for the award of contracts by any federal or state governmental agency or authority.
2. The Offeror has included, with this proposal, a certified copy of its Articles of Incorporation, and a certificate of good standing issued within one month of the date of its proposal by the State of _____. The Offeror commits to notify USTDA and the Grantee if they become aware of any change in their status in the state in which they are incorporated. USTDA retains the right to request an updated certificate of good standing.
3. Neither the Offeror nor any of its principal officers have, within the three-year period preceding this RFP, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a federal, state or local government contract or subcontract; violation of federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating federal or state criminal tax laws, or receiving stolen property.
4. Neither the Offeror, nor any of its principal officers, is presently indicted for, or otherwise criminally or civilly charged with, commission of any of the offenses enumerated in paragraph 3 above.
5. There are no federal or state tax liens pending against the assets, property or business of the Offeror. The Offeror, has not, within the three-year period preceding this RFP, been notified of any delinquent federal or state taxes in an amount that exceeds \$3,000 for which the liability remains unsatisfied. Taxes are considered delinquent if (a) the tax liability has been fully determined, with no pending administrative or judicial appeals; and (b) a taxpayer has failed to pay the tax liability when full payment is due and required.
6. The Offeror has not commenced a voluntary case or other proceeding seeking liquidation, reorganization or other relief with respect to itself or its debts under any bankruptcy, insolvency or other similar law. The Offeror has not had filed against it an involuntary petition under any bankruptcy, insolvency or similar law.

The selected Offeror shall notify the Grantee and USTDA if any of the representations included in its proposal are no longer true and correct at the time of its entry into a contract with the Grantee.

3.2.5 Subcontractor Profile

1. Name of firm and business address (street address only), including telephone and fax numbers.
2. Year established (include predecessor companies and year(s) established, if appropriate).

3.2.6 Subcontractor's Representations

If any of the following representations cannot be made, or if there are exceptions, the Subcontractor must provide an explanation.

1. Subcontractor is a corporation [*insert applicable type of entity if not a corporation*] duly organized, validly existing and in good standing under the laws of the State of _____. The subcontractor has all the requisite corporate power and authority to conduct its business as presently conducted, to participate in this proposal, and if the Offeror is selected, to execute and deliver a subcontract to the Offeror for the performance of the Technical Assistance and to perform the Technical Assistance. The subcontractor is not debarred, suspended, or to the best of its knowledge or belief, proposed for debarment or ineligible for the award of contracts by any federal or state governmental agency or authority.
2. Neither the subcontractor nor any of its principal officers have, within the three-year period preceding this RFP, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a federal, state or local government contract or subcontract; violation of federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating federal or state criminal tax laws, or receiving stolen property.
3. Neither the subcontractor, nor any of its principal officers, is presently indicted for, or otherwise criminally or civilly charged with, commission of any of the offenses enumerated in paragraph 2 above.
4. There are no federal or state tax liens pending against the assets, property or business of the subcontractor. The subcontractor, has not, within the three-year period preceding this RFP, been notified of any delinquent federal or state taxes in an amount that exceeds \$3,000 for which the liability remains unsatisfied. Taxes are considered delinquent if (a) the tax liability has been fully determined, with no pending administrative or judicial appeals; and (b) a taxpayer has failed to pay the tax liability when full payment is due and required.

5. The subcontractor has not commenced a voluntary case or other proceeding seeking liquidation, reorganization or other relief with respect to itself or its debts under any bankruptcy, insolvency or other similar law. The subcontractor has not had filed against it an involuntary petition under any bankruptcy, insolvency or similar law.

The selected subcontractor shall notify the Offeror, Grantee and USTDA if any of the representations included in this proposal are no longer true and correct at the time of the Offeror's entry into a contract with the Grantee.

3.3 ORGANIZATIONAL STRUCTURE, MANAGEMENT, AND KEY PERSONNEL

Describe the Offeror's proposed project organizational structure. Discuss how the project will be managed including the principal and key staff assignments for this Technical Assistance. Identify the Project Manager who will be the individual responsible for this project. The Project Manager shall have the responsibility and authority to act on behalf of the Offeror in all matters related to the Technical Assistance.

Provide a listing of personnel (including subcontractors) to be engaged in the project, including both U.S. and local subcontractors, with the following information for key staff: position in the project; pertinent experience, curriculum vitae; other relevant information. If subcontractors are to be used, the Offeror shall describe the organizational relationship, if any, between the Offeror and the subcontractor.

A manpower schedule and the level of effort for the project period, by activities and tasks, as detailed under the Technical Approach and Work Plan shall be submitted. A statement confirming the availability of the proposed project manager and key staff over the duration of the project must be included in the proposal.

3.4 TECHNICAL APPROACH AND WORK PLAN

Describe in detail the proposed Technical Approach and Work Plan (the "Work Plan"). Discuss the Offeror's methodology for completing the project requirements. Include a brief narrative of the Offeror's methodology for completing the tasks within each activity series. Begin with the information gathering phase and continue through delivery and approval of all required reports.

Prepare a detailed schedule of performance that describes all activities and tasks within the Work Plan, including periodic reporting or review points, incremental delivery dates, and other project milestones.

Based on the Work Plan, and previous project experience, describe any support that the Offeror will require from the Grantee. Detail the amount of staff time required by the Grantee or other participating agencies and any work space or facilities needed to complete the Technical Assistance.

3.5 EXPERIENCE AND QUALIFICATIONS

Provide a discussion of the Offeror's experience and qualifications that are relevant to the objectives and TOR for the Technical Assistance. If a subcontractor(s) is being used, similar information must be provided for the prime and each subcontractor firm proposed for the project. The Offeror shall provide information with respect to relevant experience and qualifications of key staff proposed. The Offeror shall include letters of commitment from the individuals proposed confirming their availability for contract performance.

As many as possible but not more than six (6) relevant and verifiable project references must be provided for each of the Offeror and any subcontractor, including the following information:

- Project name,
- Name and address of client (indicate if joint venture),
- Client contact person (name/ position/ current phone and fax numbers),
- Period of Contract,
- Description of services provided,
- Dollar amount of Contract, and
- Status and comments.

Offerors are strongly encouraged to include in their experience summary primarily those projects that are similar to or larger in scope than the Technical Assistance as described in this RFP.

Section 4: AWARD CRITERIA

Individual proposals will be initially evaluated by a Procurement Selection Committee of representatives from the Grantee. The Committee will then conduct a final evaluation and completion of ranking of qualified Offerors. The Grantee will notify USTDA of the best qualified Offeror, and upon receipt of USTDA's no-objection letter, the Grantee shall promptly notify all Offerors of the award and negotiate a contract with the best qualified Offeror. If a satisfactory contract cannot be negotiated with the best qualified Offeror, negotiations will be formally terminated. Negotiations may then be undertaken with the second most qualified Offeror and so forth.

The selection of the Contractor will be based on the following criteria:

The Offeror shall have experience with the following:

- Cybersecurity policy;
- Cybersecurity systems and technology;
- Information security management and control;
- Access and identity management;
- Economic benefit analysis;
- Capacity building; and
- Working experience in Africa.

The Offeror's team should consist of senior members with at least 10 years of relevant experience in the areas listed above.

Technical Approach - 25 points

The bases of the technical approach evaluation will rely on the soundness of the approach proposed by the Offeror for conducting the assessment of the current state, the gap analysis, the development of the implementation and procurement plans, documentation, and other tasks listed in the TOR. The degree to which the proposal demonstrates an understanding of the requirements will be evaluated. Additionally the feasibility and realism of the technical approach will be considered.

Management Approach - 25 points

The proposal will be evaluated on how the Offeror plans to organize staff and manage the project as well as the Offeror's planned management of consultants and subcontractors, if applicable. The Offeror's quality management plan will be also evaluated as part of the management approach.

Team Personnel - 25 points

The education, technical and managerial experience, skills, and accomplishments of the proposed personnel will be evaluated to determine the degree to which they possess the qualifications to perform their proposed role in the project. Also the proposed team's practical experience in conducting similar studies, experience in the African region, and knowledge of logistics required for effective delivery in Kenya will be considered in the evaluation.

Firm Technical Capability and Past Performance - 25 points

The Offeror's overall technical capability and past performance in similar projects, with emphasis in past performance in Africa, will be assessed. The Offeror's past performance on related projects will be evaluated to determine successful performance, quality and timeliness of delivery, proactive management and customer overall satisfaction.

Proposals that do not include all requested information may be considered non-responsive.

Price will not be a factor in selection.

ANNEX 1

Ministry of Information and Communications
Teleposta Towers, Kenyatta Ave./Koinange St.
P.O. Box 30025
Nairobi, Kenya 00100
Phone: +254-20-2251152
Fax: +254-20-315147

National Cybersecurity Master Plan. 2011-11027A

POC: Nina Patel, USTDA, 1000 Wilson Boulevard, Suite 1600, Arlington, VA 22209-3901, Tel: (703) 875-4357, Fax: (703) 875-4009. National Cybersecurity Master Plan. The Grantee invites submission of qualifications and proposal data (collectively referred to as the "Proposal") from interested U.S. firms that are qualified on the basis of experience and capability to perform technical assistance to assist the Grantee in its effort to develop a national-level plan to defend and secure Kenya's digital infrastructure.

The National Cybersecurity Master Plan will provide the Government of Kenya (GoK) with a national-level plan to defend and secure its digital infrastructure, as well as recommend minimum cybersecurity standards for the country's private networks. The Master Plan will include the development of information security management controls and procedures, cybersecurity systems, and identity and access management systems. Critically, the technical assistance also includes the development of procurement documents which take into account concepts such as total lifetime cost of ownership, reliability, scalability, quality, interoperability and conformance to international standards.

The U.S. firm selected will be paid in U.S. dollars from a \$580,000 grant to the Grantee from the U.S. Trade and Development Agency (USTDA).

A detailed Request for Proposals (RFP), which includes requirements for the Proposal, the Terms of Reference, and a background definitional mission report are available from USTDA, at 1000 Wilson Boulevard, Suite 1600, Arlington, VA 22209-3901. To request the RFP in PDF format, please go to: <https://www.ustda.gov/businessopps/rfpform.asp>. Requests for a mailed hardcopy version of the RFP may also be faxed to the IRC, USTDA at 703-875-4009. In the fax, please include your firm's name, contact person, address, and telephone number. Some firms have found that RFP materials sent by U.S. mail do not reach them in time for preparation of an adequate response. Firms that want USTDA to use an overnight delivery service should include the name of the delivery service and your firm's account number in the request for the RFP. Firms that want to send a courier to USTDA to retrieve the RFP should allow one hour after faxing the request to USTDA before scheduling a pick-up. Please note that no telephone requests for the RFP will be honored. Please check your internal fax verification receipt. Because of the large number of RFP requests, USTDA cannot respond to requests for fax verification. Requests for RFPs received before 4:00 PM will be mailed the same day.

Requests received after 4:00 PM will be mailed the following day. Please check with your courier and/or mail room before calling USTDA.

Only U.S. firms and individuals may bid on this USTDA financed activity. Interested firms, their subcontractors and employees of all participants must qualify under USTDA's nationality requirements as of the due date for submission of qualifications and proposals and, if selected to carry out the USTDA-financed activity, must continue to meet such requirements throughout the duration of the USTDA-financed activity. All goods and services to be provided by the selected firm shall have their nationality, source and origin in the U.S. or host country. The U.S. firm may use subcontractors from the host country for up to 20 percent of the USTDA grant amount. Details of USTDA's nationality requirements and mandatory contract clauses are also included in the RFP.

Interested U.S. firms should submit their Proposal in English directly to the Grantee by 5:00pm, Local (Nairobi) Time, November 18, 2011 at the above address. Evaluation criteria for the Proposal are included in the RFP. Price will not be a factor in contractor selection, and therefore, cost proposals should NOT be submitted. The Grantee reserves the right to reject any and/or all Proposals. The Grantee also reserves the right to contract with the selected firm for subsequent work related to the project. The Grantee is not bound to pay for any costs associated with the preparation and submission of Proposals.

ANNEX 2

Kenya's ICT Background Information

Kenya's ICT sector plan is based on the national priorities of poverty reduction, employment creation, human capacity development, improved governance, infrastructure development, trade promotion, industrial development and strategic partnerships as outlined in *Kenya Vision 2030*¹. *Kenya Vision 2030* is the country's development blueprint covering the period of 2008 to 2030, which is to be implemented in successive five-year medium-term plans, and which was launched by President Mwai Kibaki on October 30, 2006. Under Vision 2030, the ICT sector will be a major contributor to attaining the target of a 10% GDP growth rate by 2012, which was 4.98% in 2010, and sustaining an average 10% growth rate thereafter. This section summarizes the Kenyan ICT landscape, the main organizations and sectors, and the recent ICT developments as relating to the scope of the DM.

Kenya has made remarkable progress putting in place an ICT policy framework and implementation strategy, complete with clear measurable outcomes and timeframes. Kenya's ICT policy envisions creating an e-enabled and knowledge-based society by 2015. All aspects of Kenya's ICT sector have been growing and are expected to continue their growth positioning Kenya as a leading country in East Africa. The major growth in the last two years was in the ICT infrastructure, especially in the mobile and internet sectors and which can be attributed to competition and to the regulatory framework. The Communications Commission of Kenya (CCK) is the regulatory authority for the communications sector in Kenya. Established in 1999, by the Kenya Communications Act (KCA) No.2 of 1998, CCK's initial mandate was regulation of the telecommunications and postal/courier sub-sectors, and the management of the country's radiofrequency spectrum. In recognition of the rapid changes and developments in technology which have blurred the traditional distinctions between telecommunications, information technology (IT) and broadcasting, the Government enacted the 2009 *Kenya Communications (Amendment) Act* in January of 2009. This statute enhanced the regulatory scope and jurisdiction of CCK, and effectively transformed it to a converged regulator. CCK is now responsible for facilitating the development of the information and communications sectors (including broadcasting, multimedia, telecommunications and postal services) and e-commerce.

According to latest *CCK's ICT Sector Statistics Report*², mobile subscriptions have been steadily increasing, reaching 22 million subscribers in September 2010 with a penetration rate of 55.9%.

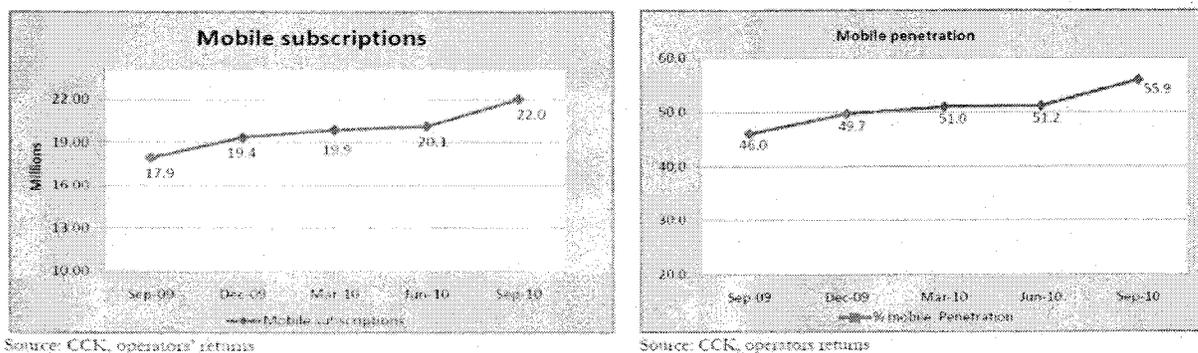
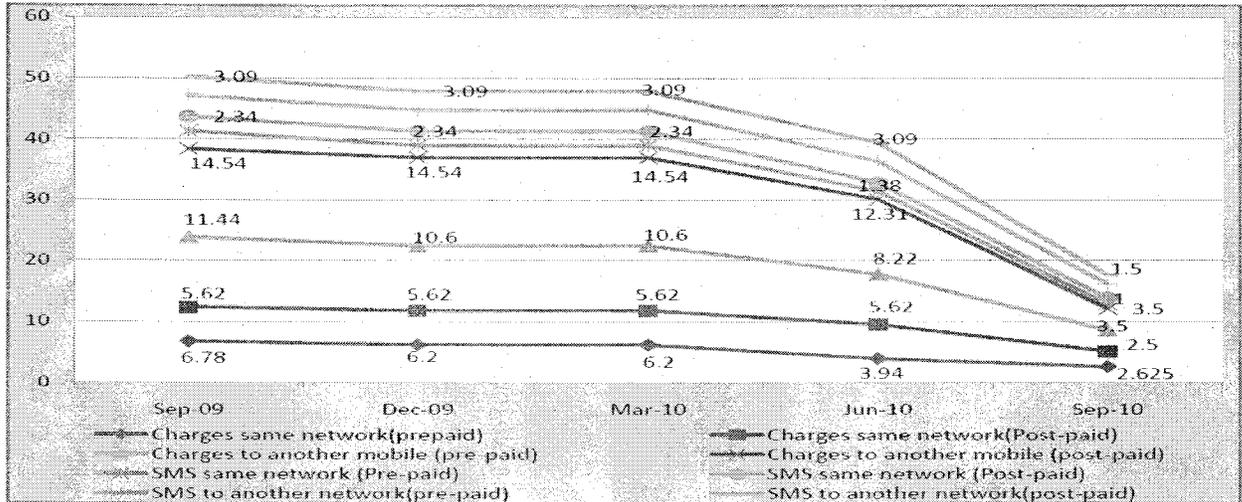


Figure 1: Mobile Subscriptions and Mobile Penetration Rate

¹ *Kenya Vision 2030 – The popular version*, Government of the Republic of Kenya, 2007

² *ICT Sector Statistics Report, 1st Quarter July-Sept 2010/2011*, Communications Commission of Kenya Final Report, Kenya ICT Projects – Kenya & Uganda ICT DM, Volume I

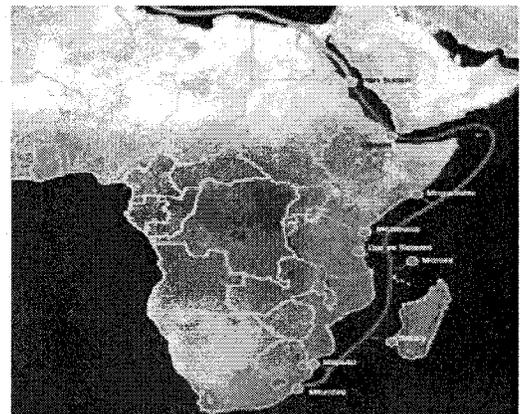
In addition to the increase in the mobile penetration rate, the mobile tariffs have also been declining significantly, over the last year, as demonstrated by Figure 2.



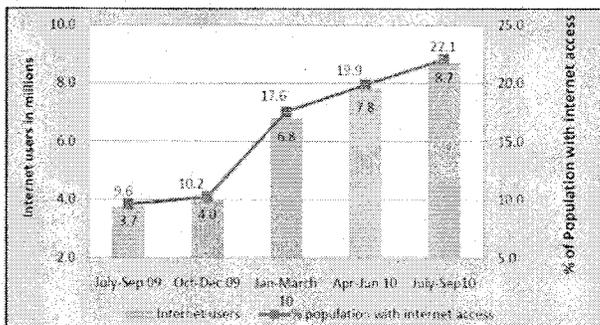
Source: CCK, Operators' returns

Figure 2: Decline of Mobile Tariffs

Regarding the internet access, the development of the privately-owned SEACOM, and the completion of the East African Submarine Cable System (EASSy), undersea fiber-optic cables in April 2010, have helped ICT technologies to leapfrog in East Africa (including Kenya), by dramatically increasing connectivity and drastically reducing prices for ICT services.



This development resulted in doubling the number of internet users from 3.7 million users in September 2009 to 8.7 million users in September 2010. These numbers, in Figure 4, show that the population percentage with internet access increased from 9.6% to 22.1% during the period from 09/2009-09/2010.



Source: CCK, Operators' returns

Figure 3: EASSy and SEACOM Cables

Figure 4: Percentage of Population with Internet Access

In summary the SWOT Analysis, as published by the MoIC in its *ICT National Strategic Master Plan for 2008-2012*³, provides a good snapshot about the Strengths, Weakness, Opportunities and Threats of the ICT sector in Kenya.

<p style="text-align: center;">Strengths</p> <ul style="list-style-type: none"> • Harmonized provisions of information and communications services. • Specialized and reputable organization providing specific information and communication services. • Existence of legal framework to regulate the ICT sector. • Qualified and experienced staff. • Ability to synergize with other sectors of the Economy. • National network for news-gathering and dissemination that increases universal access to information. 	<p style="text-align: center;">Weaknesses</p> <ul style="list-style-type: none"> • Inadequate and outdated equipment. • Inadequate capital and human resources. • Weak and obsolete policy, legal and regulatory framework for the sector. • Inadequate institutional and technical capacity. • Bureaucratic Procedures. • Poor remuneration. • Lack of organized information and communication data bank. • Poor governance
<p style="text-align: center;">Opportunities</p> <ul style="list-style-type: none"> • Restructuring in the Public Service. • Liberalization and Privatization of the sector. • Increased use of information and communication technology. • External support • Increased Stakeholders participation. • Enhanced Capacity building for the sector. • Enormous and untapped potential of the ICT industry. 	<p style="text-align: center;">Threats</p> <ul style="list-style-type: none"> • Brain drain of technical staff. • Negative portrayal of the country's image abroad. • General insecurity reducing investment opportunity. • Rapid changes in technology and market needs. • Regional compensation from more technologically advanced countries.

Figure 7: Extracted from SWOT Analysis for the ICT Sector in Kenya⁴

Kenya National Cybersecurity Master Plan

1.1 Executive Summary

The Government of Kenya seeks assistance from USTDA for technical assistance to develop a National Cybersecurity Master Plan. Kenya's connection to the internet was greatly enhanced with

³ Kenya ICT Strategic Policy Plan for 2008-2012

⁴ Kenya ICT Strategic Policy Plan for 2008-2012

Final Report, Kenya ICT Projects – Kenya & Uganda ICT DM, Volume I

the connection of the SEACOM⁵ cable in the summer of 2009 and the connection of the EASSy cable in 2010. With the increased connectivity came also the rise in cyber crime in Kenya. There are currently serious loopholes in the systems, as it has been evident that it is common practice by most firms not to factor the possible security risks while setting up their systems. The probability of risk is increasing with fiber connectivity and the increased use of technology by the GoK. This problem is not restricted only to the government but also to the private sector, especially the financial and telecommunications sectors. With mounting evidence of increasing vulnerabilities, the GoK and leaders in the private sector need to make improvements to their cybersecurity infrastructure. Private and public organizations are required to invest in security systems to protect hackers from accessing their networks, systems and data.

Kenya started to take some initiatives to address the cybersecurity threats, however these initiatives are in their very early stages, fragmented and lack a national level plan that can address the cybersecurity threat holistically, at both strategy and implementation levels.

1.2 Project Description

The years of 2009 and 2010 marked key milestones in the national connectivity of Kenya with the building of undersea cables and national terrestrial infrastructure. These kinds of connections opened Kenya to a whole new world of networks and information sharing, on both regional and international levels. With this, Kenya is becoming more exposed to cyber criminals. Recently there has been an increased number of websites that were compromised, including the websites of the Ministry of Finance (www.statehouse.co.ke), the Kenya Administration Police (administrationpolice.go.ke), the Kenya Government Portal (kenya.go.ke), and the mobile phone company YU (yu.co.ke).

Moreover, the GoK has a very ambitious plan for implementing e-government, shared services and a shift to the national data paradigm, also referred to as government data centers, and cloud computing. In May 2011, the Kenya ICT Board announced and launched *Kenya's Shared Service Master Plan*, which will implement a wide range of e-government services. With the increased connectivity and Kenya's ambitious e-government plan, the level of cybersecurity threat escalates even more. The Ministry of Information and Communication's (MoIC) Permanent Secretary, Dr. Bitange Ndemo, emphasized that cybersecurity is a major and critical issue in Kenya, which must be addressed urgently.

To address the cybersecurity issue, the GoK has started to take some initiatives, which can be summarized as follows:

- Provisions enshrined in the Kenya Communications (Amendment) Act of 2009, which mandates the Communications Commission of Kenya (CCK), Kenya's national ICT regulatory authority, to develop Kenya's *National Electronic Transactions Framework*;
- Establishing a national computer emergency response team (CERT) known as the *Kenya Computer Emergency Response Team (KE-CERT)*. The national CERT will coordinate responses to cybersecurity incidents at the national level and cooperate with regional and international entities involved with the management of cybersecurity incidents. CERT constituency will be comprised of relevant stakeholders. CERT Services are mandated to be: proactive, reactive, artifact handling, capacity building/awareness and including R&D;

⁵ SEACOM is a privately funded venture which built, owns, and operates a submarine fiber-optic cable connecting communication carriers in south and east Africa.

- Establishing the *National Certification Authority Framework*, that is to provide the platform for the provision of digital certificates in Kenya;
- Partnering with the International Telecommunication Union (ITU) in the area of cybersecurity management through the *International Multi-stakeholder Partnership against Cyber Threats (IMPACT)*;
- Participating and chairing the East Africa Communications Organization (EACO) Cybersecurity Taskforce. The EACO Cybersecurity taskforce was formed in 2008 to coordinate the development of a cybersecurity management framework for the EACO region, and includes members from the five East African Countries: Tanzania, Uganda, Burundi, Rwanda, and Kenya; and
- Planning to procure a public key infrastructure (PKI) solution for the GoK.

However, most of the above initiatives are still in their early stages, isolated and reactive in nature. To that end, the Government of Kenya seeks assistance from USTDA for technical assistance to develop their *National Cybersecurity Master Plan*, which will have a whole-of-government approach to cybersecurity at both the strategy and implementation levels. The GoK, represented by the MoIC, is currently addressing the cybersecurity threat and would like to capitalize on the U.S.'s experience and knowledge in developing a national cybersecurity master plan for Kenya.

The National Cybersecurity Master Plan is to provide the GoK with a national level plan to defend Kenya's information and communications infrastructure and to develop a comprehensive approach to securing its digital infrastructure. The National Cybersecurity Master Plan shall establish an approach that the GoK is to take in identifying current and emerging cyber threats, shoring up current and future telecommunications and cyber vulnerabilities, and responding to or proactively addressing entities that wish to steal or manipulate protected data on secure government systems.

The National Cybersecurity Master Plan shall include both the high-level strategy plan and the detailed implementation and procurement plans for various short and mid-term initiatives, which the GoK should implement to secure its cyberspace. The main goals of the *National Cybersecurity Plan* can be summarized in the following:

- Establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the GoK, and ultimately with local governments and private sector partners, and the ability to act quickly to reduce Kenya current vulnerabilities and prevent intrusions;
- Strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the GoK; and working to define and develop strategies to deter hostile or malicious activity in cyberspace;
- Establish a comprehensive national security strategy for cyberspace;
- Identify governance and responsibility for cybersecurity and establish Kenya's leadership for cybersecurity in East Africa;
- Set and enforce the minimum required standards for securing cyberspace, and ensure that the delivery of critical services can continue when they are attacked;
- Use acquisitions policies and rule to drive security, to encourage the development and use of products and services that are secure, based on standards and guidelines developed in partnership with industry;
- Build human capital and improved technologies for securing cyberspace by expanding research, training and education;

- Strengthen the public-private partnerships in cybersecurity; and
- Establish a trusted digital identities framework, which is critical for improving the security of online transactions, and mandate strong authentication for access to critical infrastructure.

The National Cybersecurity Plan shall consider both the Government of Kenya and the private sectors, to ensure an organized and unified response to cyber incidents; strengthen public/private partnerships to find technology solutions that ensure security; invest in both capacity building and technology necessary to meet the cybersecurity challenges; and begin a campaign to promote cybersecurity awareness and digital literacy. The plan's proposed actions shall be conducted in a way that is consistent with ensuring the privacy rights of the citizens.

The development of a comprehensive national cybersecurity master plan will require the Contractor to perform a various set of activities which should include, at minimum, the following:

- Review of Kenya's regulatory, policy and legal framework;
- Identification of critical cyber assets and a comprehensive cybersecurity assessment;
- Development of information security management control policy and procedures;
- Identification of required cybersecurity technology systems;
- Development of a trusted identity framework;
- Development of the cybersecurity organizational structure and governance;
- Development of the cybersecurity human capital and training plan;
- Identifying cybersecurity short- and mid-term initiatives and develop their implementation and procurement plans;
- Develop a cybersecurity awareness campaign and workshops;
- Perform economic and financial Analysis; and
- Prepare the Final Report to include the *Comprehensive National Cybersecurity Master Plan*.

This project is expected to significantly improve the protection of Kenya's cyber assets and present significant export opportunity for U.S. companies, which specialize in information security products and services.

1.3 Project Sponsor's Capabilities and Commitment

The proposed sponsor for this project will be the Kenya Ministry of Information and Communication (MOIC), under the auspices of Permanent Secretary Dr. Bitange Ndemo.

The Kenyan MoIC was constituted in June 2004 with the aim of creating a one-stop shop for all ICT related government activities. The Ministry is composed of two major sub-sectors, the Information and Broadcasting sub-sector and the Communications sub-sector. The Information and Broadcasting sub-sector is responsible for the gathering and dissemination of news and information. The Communications sub-sector comprises the telecommunications, the information communications technologies (ICTs), and the postal services. In its current form, the Ministry is a one-stop shop that covers all ICT activities including the administration of information and communications technologies, policy formulation and implementation, regulatory, infrastructure development and human resource management.

During the last period, MoIC's main objectives focused on creating cost-effective telecommunication services. To this end, the GoK instated major policy measures to encourage competition and increase ICT investments. Some of the major accomplishments included:

- Liberalization of the International Gateway;
- Launch of the National ICT Policy and Strategy;
- Launch of the Kenya ICT Board;
- Development of ICT Strategy for Business Process;
- Construction of fiber cable network;
- Privatization of Telkom;
- Establishment of Universal Access Fund; and
- Lowered and/or abolished taxes on ICT equipment and services.

MoIC has a proven track record in successful implementation of ICT projects across all of the GoK and is fully capable of implementing and sponsoring this project.

1.4 Implementation Financing

Both the GoK and the private sector are fully aware that investing in cybersecurity is essential in the next phase and is no longer considered as an elective but rather a vital and crucial investment. It is expected that the GoK will make a direct investment in cybersecurity from its national budget.

Despite the general resource limitations, the Kenya Treasury has prioritized resources towards ICT development. In 2010 and 2011 the research, innovation and technology sector was allocated \$828 million, up from \$568 million in 2009/2010. The allocation projection for 2011/12 is set at \$855 million and for 2012/2013 \$900 million.⁶

The allocated funds are being used to fund projects and activities under the following programs, in the order of their priority, during the 2010/11 Financial Year:

- Human resource development;
- ICT infrastructure development;
- Research and innovation;
- Information and communication services;
- Data management; and
- Development of policy, legal and institutional framework.

Cybersecurity implementation should be part of the ICT infrastructure development, information and communication services, and data management programs. Hence, ICT infrastructure development can be funded through funds allocated to these programs, by both the GoK and the World Bank (KTCIP).

Moreover, it is also expected that the *National Cybersecurity Master Plan* will increase the cybersecurity spending by the private sector, specifically the mobile companies and banking sectors. The National Cybersecurity Master Plan will mandate the minimum set of security standards and

⁶ "Providing an Enabling Environment for ICT Development", Joseph Kinyua, Permanent Secretary Treasury, Connecting government Conference Mombasa, April 19, 2011
Final Report, Kenya ICT Projects – Kenya & Uganda ICT DM, Volume I

measure to be in place by the financial and the private sector to protect customer data and protect their cyber assets. Implementing these security measures will increase private sector spending and investment in cybersecurity.

1.5 U.S. Export Potential

The potential investment is almost “infinitely expandable” over time as more e-government projects are implemented. It is estimated that required GoK investment required to implement the National Cybersecurity Master Plan will be in the range of \$20 million to \$30 million over the next three to five years. In addition to GoK’s investment, the cybersecurity and data protection policies, which are expected as a result of this TA, will result in additional investment by the private sector in order to comply with these policies.

It is anticipated that a large percentage of the project will be implemented by U.S. companies as a result of the U.S. companies’ leading position in the field of cybersecurity. It is premature to provide an accurate estimate of the U.S. exports’ potential prior to the development of the cybersecurity master plan. However, a preliminary estimate of the U.S. export potential is likely to be in the range of \$15 million to \$20 million out of the \$20 million to \$30 million estimated total project implementation cost. This amount of U.S. export potential may be resulting from the anticipated export of the following types of U.S. products and services:

- ***Cybersecurity Products/Systems:***

Cybersecurity products and systems, needed to implement the National Cybersecurity Master Plan, present excellent U.S. export potential, with products such as antivirus software, firewalls, intrusion detection, identity management, access control, identification and authentication, vulnerability, scanners, hardware products, etc. It is expected that Kenya’s National Cybersecurity Plan will identify needed cybersecurity products, likely to be in the range of \$5 million to \$10 million, to protect Kenya’s cyber assets and to put in place adequate cybersecurity measures. U.S. companies possess a leading edge and are world-renowned for their cybersecurity expertise and products.

- ***System Integration, Consulting and Related Professional Services:***

In addition to the cost of the cybersecurity products, hardware and software, the design and deployment of the cybersecurity systems will require services from experienced system integrators and consulting companies to deliver the design, deployment and training of these cybersecurity systems. It is expected that the cost of the implementation and training of these systems will be in the range between \$10 million to \$15 million. Several U.S. system integrators and consulting companies possess extensive and unique experience in the design and implementation of cybersecurity solutions.

- ***Training and Capacity Building:***

The U.S. provides excellent training and capacity building opportunities, with its countless well-known companies, distinguished universities and recognized centers of excellence, which positions the U.S. in the front-line to assist the GoK in the building of its cybersecurity workforce. It is expected that the cost of cybersecurity training and capacity building in this field, including building CERT and CSIRT capability, will be in the range of \$5 million over the next five year period.

Project Component	Estimated Implementation Cost	Estimated U.S. Export Potential
Cybersecurity Products/ Systems	\$5 million - \$10 million	\$4 million - \$6 million
System Integration, Consulting and Related Professional Services	\$10 million - \$15 million	\$8 million - \$10 million
Training and Capacity Building	\$5 million	\$3 million - \$4 million
Total	\$20 million - \$30 million	\$15 million - \$20 million

Table 1: Estimated U.S. Export Potential for the Cybersecurity Project

1.6 Foreign Competition and Market Entry Issues

The U.S. cybersecurity technology and consulting services are very well-positioned in Kenya with the United States being regarded as a leader in this field and is favored by GoK officials. However, we cannot underestimate the effect of the procurement laws and practice, which extensively favor extensively the lowest bidder whilst putting less emphasis on the reliability, scalability, and maintainability of the product. Korean companies are trying to position themselves in this growing market and, are currently in discussion with the MoIC to implement Public Key Infrastructure (PKI) solutions for the GoK. Other foreign companies active in Kenya in this field are:

- LG CNS based in Seoul, Korea, which has been awarded recently a \$3.4 million contract to establish a cybersecurity center in Morocco,
- Huawei based in China,
- ENTIRETEC AG based in Germany, and
- Aujas based in India.

In recognition of the U.S. leadership in the cybersecurity technology domain, the MoIC is currently working with the U.S. Commercial Services in Nairobi to establish an MOU between the GoK and the USG for collaboration in the cybersecurity space. This MOU will also provide a legitimate basis for the MoIC to limit the competition in some of the future cybersecurity procurements to U.S. companies solely, if they decided that U.S. technology is in the best interest of the GoK.

The USTDA Cybersecurity Reverse Trade Mission, of November 2010, favorably contributed in positioning U.S. technology in this regard. Furthermore, USTDA’s assistance in developing the *Kenya Cybersecurity Master Plan* will not only strengthen but also reinforce this position across all the different GoK ministries and in the private sector, especially the financial and telecommunication sectors.

RGITC has contacted several interested U.S. companies, large U.S. companies as well as small businesses, and they have all shown a very strong interest in supporting Kenya’s cybersecurity need. Moreover, based on discussions with the companies and the GoK, it has been evidenced to RGITC that U.S. companies are very well-positioned to provide products and services.

1.7 Development Impact

The National Cybersecurity Master plan, if implemented, will have a significant developmental impact on Kenya particularly on the following areas:

Human Capacity Building

Kenya is in a great need to build its cybersecurity workforce. The National Cybersecurity Master Plan will address the human capacity building aspects and will provide detailed plans to build and train the cybersecurity workforce. It is also expected that each government agency and local authority (LA) will be staffed with information security personnel as part of their ICT departments. Additionally, information and cybersecurity personnel are expected to be required at organizations with a national mandate such as the CERT, CCK, and MoIC.

Technology Transfer and Productivity Improvement

If implemented, Kenya will tremendously benefit from the U.S. technology and advances in cybersecurity. Implementing these systems will prevent loss in productivity that would result as a consequence of any security breach. As Kenya is planning to offer more on-line services, any security threat may have a huge impact on the availability of these services and can result in a significant negative impact on productivity.

Market-Oriented Reform

The National Cybersecurity Master Plan will address regulation, laws, and policy related to cybersecurity, such as trusted cyber identities and e-signature. The implementation of the plan will result in removing the barriers slowing down e-commerce adoption and will strengthen international trade.

Infrastructure

The implementation of this project does not include developing any new infrastructure to Kenya. However, it is aimed to protect the existing information and communication infrastructure and ensure their availability. This protection is considered equally important as building a new infrastructure.

Others

The implementation of adequate cybersecurity measures and systems will increase the trust in utilizing on-line services and transactions, mainly for government and on-line financial services. These will help in expanding e-commerce and the Kenyan economy.

1.8 Impact on the Environment

There is no expected negative impact on the environment from the cybersecurity project as this project entails the procurement of hardware and software, and knowledge transfer in the field of cybersecurity. The knowledge transfer and software components of this project have no impact on the environment. The hardware component of this project is in line with the on-going maintenance and deposition of ICT equipment and is expected to have negligible impact on the environment, if any.

1.9 Impact on U.S. Labor

This project will assist the Government of Kenya (GoK) to protect its cyber assets. The project is therefore not expected to have any negative impact on the U.S. industry. It is also not expected to

reduce employment in the U.S. On the other hand, if the project is implemented, positive impact on the U.S. labor, resulting from the U.S. exports and in the form of jobs in the ICT industry is anticipated.

We see no evidence to suggest that any aspect of the project would contravene the Foreign Operations, Export Financing and Related Programs Appropriates legislation. Based upon our review, we found that the project does not provide:

- any financial incentives to a business enterprise currently located in the United States for the purpose of inducing such an enterprise to relocate outside the United States if such incentive or inducement is likely to reduce the number of employees of such business enterprise in the United States because United States production is being replaced by such enterprise outside the United States;
- assistance for any project or activity that contributes to the violation of internationally recognized workers' rights; or
- direct assistance for establishing or expanding production of any commodity for export by any country other than the United States, if the commodity is likely to be in surplus on world markets at the time the resulting productive capacity is expected to become operative and if the assistance will cause substantial injury to United States producers of the same, similar, or competing commodity.

1.10 Justification

Justification for the USTDA grant funding is based on the following factors:

- U.S. companies offer compelling technology and professional solutions that address Kenya's ICT needs. Exports related to this project, over the next three to five years are anticipated to reach \$20 million to \$30 million;
- Korean and other suppliers are aggressively trying to enter this market space. USTDA's involvement can have a great impact in enforcing U.S. leadership and assisting the GoK in defining and developing the technical specifications and procurement documents that will put emphasis on the best value to the GoK taking into consideration standards and interoperability, reliability, and effectiveness of the solutions. This will be to the benefit of U.S. companies by allowing for a fair competition considering all aspects of the solution, and not just the initial cost ; and
- The USTDA funding for this technical assistance will fill an existing critical gap, and is much needed to support the tremendous and successful efforts by the GoK in its e-government initiatives as well as the private sector's ICT efforts.

1.11 Recommendations

In summary, RGITC recommends USTDA funding for the *Kenya National Cybersecurity Master Plan* as the project meets the USTDA funding criteria summarized as follows:

- The implementation of National Cybersecurity Master Plan has a high probability of receiving implementation financing from the GoK's national budget, the World Bank, and the private sector.
- The project represents an opportunity for sales of U.S. goods and services in the range from \$20 million to \$30 million

- The project is a top priority for the project sponsor, the Ministry of Information and Communication and for the GoK. The project also supports the recent White House *International Strategy for Cyber Space*, launched on May 16, 2011 which indicates international development and capacity building as one of the policy's top priorities. The policy indicates that the U.S. will provide the necessary knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity.

ANNEX 3



U.S. TRADE AND DEVELOPMENT AGENCY
Arlington, VA 22209-2131

NATIONALITY, SOURCE, AND ORIGIN REQUIREMENTS

The purpose of USTDA's nationality, source, and origin requirements is to assure the maximum practicable participation of American contractors, technology, equipment and materials in the prefeasibility, feasibility, and implementation stages of a project.

USTDA STANDARD RULE (GRANT AGREEMENT STANDARD LANGUAGE):

Except as USTDA may otherwise agree, each of the following provisions shall apply to the delivery of goods and services funded by USTDA under this Grant Agreement: (a) for professional services, the Contractor must be either a U.S. firm or U.S. individual; (b) the Contractor may use U.S. subcontractors without limitation, but the use of subcontractors from host country may not exceed twenty percent (20%) of the USTDA Grant amount and may only be used for specific services from the Terms of Reference identified in the subcontract; (c) employees of U.S. Contractor or U.S. subcontractor firms responsible for professional services shall be U.S. citizens or non-U.S. citizens lawfully admitted for permanent residence in the U.S.; (d) goods purchased for implementation of the Study and associated delivery services (e.g., international transportation and insurance) must have their nationality, source and origin in the United States; and (e) goods and services incidental to Study support (e.g., local lodging, food, and transportation) in host country are not subject to the above restrictions. USTDA will make available further details concerning these standards of eligibility upon request.

NATIONALITY:

1) Rule

Except as USTDA may otherwise agree, the Contractor for USTDA funded activities must be either a U.S. firm or a U.S. individual. Prime contractors may utilize U.S.

subcontractors without limitation, but the use of host country subcontractors is limited to 20% of the USTDA grant amount.

2) Application

Accordingly, only a U.S. firm or U.S. individual may submit proposals on USTDA funded activities. Although those proposals may include subcontracting arrangements with host country firms or individuals for up to 20% of the USTDA grant amount, they may not include subcontracts with third country entities. U.S. firms submitting proposals must ensure that the professional services funded by the USTDA grant, to the extent not subcontracted to host country entities, are supplied by employees of the firm or employees of U.S. subcontractor firms who are U.S. individuals.

Interested U.S. firms and consultants who submit proposals must meet USTDA nationality requirements as of the due date for the submission of proposals and, if selected, must continue to meet such requirements throughout the duration of the USTDA-financed activity. These nationality provisions apply to whatever portion of the Terms of Reference is funded with the USTDA grant.

3) Definitions

A "U.S. individual" is (a) a U.S. citizen, or (b) a non-U.S. citizen lawfully admitted for permanent residence in the U.S. (a green card holder).

A "U.S. firm" is a privately owned firm which is incorporated in the U.S., with its principal place of business in the U.S., and which is either (a) more than 50% owned by U.S. individuals, or (b) has been incorporated in the U.S. for more than three (3) years prior to the issuance date of the request for proposals; has performed similar services in the U.S. for that three (3) year period; employs U.S. citizens in more than half of its permanent full-time positions in the U.S.; and has the existing capability in the U.S. to perform the work in question.

A partnership, organized in the U.S. with its principal place of business in the U.S., may also qualify as a "U.S. firm" as would a joint venture organized or incorporated in the United States consisting entirely of U.S. firms and/or U.S. individuals.

A nonprofit organization, such as an educational institution, foundation, or association may also qualify as a "U.S. firm" if it is incorporated in the United States and managed by a governing body, a majority of whose members are U.S. individuals.

SOURCE AND ORIGIN:

1) Rule

In addition to the nationality requirement stated above, any goods (e.g., equipment and materials) and services related to their shipment (e.g., international transportation and insurance) funded under the USTDA Grant Agreement must have their source and origin in the United States, unless USTDA otherwise agrees. However, necessary purchases of goods and project support services which are unavailable from a U.S. source (e.g., local food, housing and transportation) are eligible without specific USTDA approval.

2) Application

Accordingly, the prime contractor must be able to demonstrate that all goods and services purchased in the host country to carry out the Terms of Reference for a USTDA Grant Agreement that were not of U.S. source and origin were unavailable in the United States.

3) Definitions

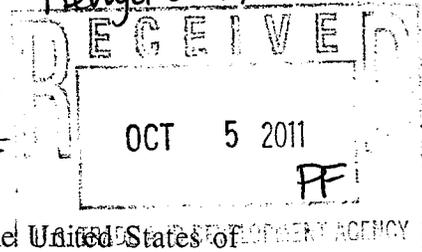
"Source" means the country from which shipment is made.

"Origin" means the place of production, through manufacturing, assembly or otherwise.

Questions regarding these nationality, source and origin requirements may be addressed to the USTDA Office of General Counsel.

ANNEX 4

Kenya 2011-11027A



JW
LZ

GRANT AGREEMENT

This Grant Agreement is entered into between the Government of the United States of America, acting through the U.S. Trade and Development Agency ("USTDA") and the Government of the Republic of Kenya, acting through the Ministry of Information and Communications ("Grantee"). USTDA agrees to provide the Grantee under the terms of this Agreement US\$580,000 ("USTDA Grant") to fund the cost of goods and services required for technical assistance ("TA") on the proposed National Cybersecurity Master Plan ("Project") in Kenya ("Host Country").

PM JJ
JM MB
LB KM
PD SU
RY AY

1. USTDA Funding

The funding to be provided under this Grant Agreement shall be used to fund the costs of a contract between the Grantee and the U.S. firm selected by the Grantee ("Contractor") under which the Contractor will perform the TA ("Contract"). Payment to the Contractor will be made directly by USTDA on behalf of the Grantee with the USTDA Grant funds provided under this Grant Agreement.

2. Terms of Reference

The Terms of Reference for the TA ("Terms of Reference") are attached as Annex I and are hereby made a part of this Grant Agreement. The TA will examine the technical, financial, and other critical aspects of the proposed Project. The Terms of Reference for the TA shall also be included in the Contract.

3. Standards of Conduct

USTDA and the Grantee recognize the existence of standards of conduct for public officials, and commercial entities, in their respective countries. The parties to this Grant Agreement and the Contractor shall observe these standards, which include not accepting payment of money or anything of value, directly or indirectly, from any person for the purpose of illegally or improperly inducing anyone to take any action favorable to any party in connection with the TA.

4. Grantee Responsibilities

The Grantee shall undertake its best efforts to provide reasonable support for the Contractor, such as local transportation, office space, and secretarial support.

5. USTDA as Financier

(A) USTDA Approval of Competitive Selection Procedures

Selection of the U.S. Contractor shall be carried out by the Grantee according to its established procedures for the competitive selection of contractors with advance notice of the procurement published online through *Federal Business Opportunities* (www.fedbizopps.gov). Upon request, the Grantee will submit these contracting procedures and related documents to USTDA for information and/or approval.

(B) USTDA Approval of Contractor Selection

The Grantee shall notify USTDA at the address of record set forth in Article 17 below upon selection of the Contractor to perform the TA. Upon approval of this selection by USTDA, the Grantee and the Contractor shall then enter into a contract for performance of the TA. The Grantee shall notify in writing the U.S. firms that submitted unsuccessful proposals to perform the TA that they were not selected.

(C) USTDA Approval of Contract Between Grantee and Contractor

The Grantee and the Contractor shall enter into a contract for performance of the TA. This contract, and any amendments thereto, including assignments and changes in the Terms of Reference, must be approved by USTDA in writing. To expedite this approval, the Grantee (or the Contractor on the Grantee's behalf) shall transmit to USTDA, at the address set forth in Article 17 below, a photocopy of an English language version of the signed contract or a final negotiated draft version of the contract.

(D) USTDA Not a Party to the Contract

It is understood by the parties that USTDA has reserved certain rights such as, but not limited to, the right to approve the terms of the contract and any amendments thereto, including assignments, the selection of all contractors, the Terms of Reference, the Final Report, and any and all documents related to any contract funded under the Grant Agreement. The parties hereto further understand and agree that USTDA, in reserving any or all of the foregoing approval rights, has acted solely as a financing entity to assure the proper use of United States Government funds, and that any decision by USTDA to exercise or refrain from exercising these approval rights shall be made as a financier in the course of funding the TA and shall not be construed as making USTDA a party to the contract. The parties hereto understand and agree that USTDA may, from time to time, exercise the foregoing approval rights, or discuss matters related to these rights and the Project with the parties to the contract or any subcontract, jointly or separately, without thereby incurring any responsibility or liability to such parties. Any approval or failure to approve by USTDA shall not bar the Grantee or USTDA from asserting any right they might have against the

Contractor, or relieve the Contractor of any liability which the Contractor might otherwise have to the Grantee or USTDA.

(E) Grant Agreement Controlling

Regardless of USTDA approval, the rights and obligations of any party to the contract or subcontract thereunder must be consistent with this Grant Agreement. In the event of any inconsistency between the Grant Agreement and any contract or subcontract funded by the Grant Agreement, the Grant Agreement shall be controlling.

6. Disbursement Procedures

(A) USTDA Approval of Contract Required

USTDA will make disbursements of Grant funds directly to the Contractor only after USTDA approves the Grantee's contract with the Contractor.

(B) Contractor Invoice Requirements

The Grantee should request disbursement of funds by USTDA to the Contractor for performance of the TA by submitting invoices in accordance with the procedures set forth in the USTDA Mandatory Clauses in Annex II.

7. Effective Date

The effective date of this Grant Agreement ("Effective Date") shall be the date of signature by both parties or, if the parties sign on different dates, the date of the last signature.

8. TA Schedule

(A) TA Completion Date

The completion date for the TA, which is September 20, 2013, is the date by which the parties estimate that the TA will have been completed.

(B) Time Limitation on Disbursement of USTDA Grant Funds

Except as USTDA may otherwise agree, (a) no USTDA funds may be disbursed under this Grant Agreement for goods and services which are provided prior to the Effective Date of the Grant Agreement; and (b) all funds made available under the Grant Agreement must be disbursed within four (4) years from the Effective Date of the Grant Agreement.

9. USTDA Mandatory Clauses

All contracts funded under this Grant Agreement shall include the USTDA mandatory clauses set forth in Annex II to this Grant Agreement. All subcontracts funded or partially funded with USTDA Grant funds shall include the USTDA mandatory clauses, except for clauses B(1), G, H, I, and J.

10. Use of U.S. Carriers

(A) Air

Transportation by air of persons or property funded under the Grant Agreement shall be on U.S. flag carriers in accordance with the Fly America Act, 49 U.S.C. 40118, to the extent service by such carriers is available, as provided under applicable U.S. Government regulations.

(B) Marine

Transportation by sea of property funded under the Grant Agreement shall be on U.S. carriers in accordance with U.S. cargo preference law.

11. Nationality, Source and Origin

Except as USTDA may otherwise agree, the following provisions shall govern the delivery of goods and services funded by USTDA under the Grant Agreement: (a) for professional services, the Contractor must be either a U.S. firm or U.S. individual; (b) the Contractor may use U.S. subcontractors without limitation, but the use of subcontractors from Host Country may not exceed twenty percent (20%) of the USTDA Grant amount and may only be used for specific services from the Terms of Reference identified in the subcontract; (c) employees of U.S. Contractor or U.S. subcontractor firms responsible for professional services shall be U.S. citizens or non-U.S. citizens lawfully admitted for permanent residence in the U.S.; (d) goods purchased for performance of the TA and associated delivery services (e.g., international transportation and insurance) must have their nationality, source and origin in the United States; and (e) goods and services incidental to TA support (e.g., local lodging, food, and transportation) in Host Country are not subject to the above restrictions. USTDA will make available further details concerning these provisions upon request.

12. Taxes

USTDA funds provided under the Grant Agreement shall not be used to pay any taxes, tariffs, duties, fees or other levies imposed under laws in effect in Host Country. Neither the Grantee nor the Contractor will seek reimbursement from USTDA for such taxes, tariffs, duties, fees or other levies.

13. Cooperation Between Parties and Follow-Up

The parties will cooperate to assure that the purposes of the Grant Agreement are accomplished. For five (5) years following receipt by USTDA of the Final Report (as defined in Clause I of Annex II), the Grantee agrees to respond to any reasonable inquiries from USTDA about the status or results of the Project, and upon receipt by the Grantee of the Final Report, will designate (by both title and organization) a point of contact for any such inquiries.

14. Implementation Letters

To assist the Grantee in the implementation of the TA, USTDA may, from time to time, issue implementation letters that will provide additional information about matters covered by the Grant Agreement. The parties may also use jointly agreed upon implementation letters to confirm and record their mutual understanding of matters covered by the Grant Agreement.

15. Recordkeeping and Audit

The Grantee agrees to maintain books, records, and other documents relating to the TA and the Grant Agreement adequate to demonstrate implementation of its responsibilities under the Grant Agreement, including the selection of contractors, receipt and approval of contract deliverables, and approval or disapproval of contractor invoices for payment by USTDA. Such books, records, and other documents shall be separately maintained for three (3) years after the date of the final disbursement by USTDA. The Grantee shall afford USTDA or its authorized representatives the opportunity at reasonable times to review books, records, and other documents relating to the TA and the Grant Agreement.

16. Representation of Parties

For all purposes relevant to the Grant Agreement, the Government of the United States of America will be represented by the U. S. Ambassador to Host Country or USTDA and Grantee will be represented by the Permanent Secretary. The parties hereto may, by written notice, designate additional representatives for all purposes under the Grant Agreement.

17. Addresses of Record for Parties

Any notice, request, document, or other communication submitted by either party to the other under the Grant Agreement shall be in writing or through a wire or electronic medium which produces a tangible record of the transmission, such as a telegram, cable or facsimile, and will be deemed duly given or sent when delivered to such party at the following:

To: Ministry of Information and Communications
Teleposta Towers, Kenyatta Ave./Koinange St.

P.O. Box 30025
Nairobi
Kenya
00100

Phone: +254-20-2251152
Fax: +254-20-315147

To: U.S. Trade and Development Agency
1000 Wilson Boulevard, Suite 1600
Arlington, Virginia 22209-3901
USA

Phone: (703) 875-4357
Fax: (703) 875-4009

All such communications shall be in English, unless the parties otherwise agree in writing. In addition, the Grantee shall provide the Commercial Section of the U.S. Embassy in Host Country with a copy of each communication sent to USTDA.

Any communication relating to this Grant Agreement shall include the following fiscal data:

Appropriation No.: 11 11/12 1001
Activity No.: 2011-11027A
Reservation No.: 2011278
Grant No.: GH201111278

18. Termination Clause

Either party may terminate the Grant Agreement by giving the other party thirty (30) days advance written notice. The termination of the Grant Agreement will end any obligations of the parties to provide financial or other resources for the TA, except for payments which they are committed to make pursuant to noncancellable commitments entered into with third parties prior to the written notice of termination.

19. Non-waiver of Rights and Remedies

No delay in exercising any right or remedy accruing to either party in connection with the Grant Agreement shall be construed as a waiver of such right or remedy.

20. U.S. Technology and Equipment

By funding this TA, USTDA seeks to promote the Project objectives of the Host Country through the use of U.S. technology, goods, and services. In recognition of this purpose, the Grantee agrees that it will allow U.S. suppliers to compete in the procurement of technology, goods and services needed for Project implementation.

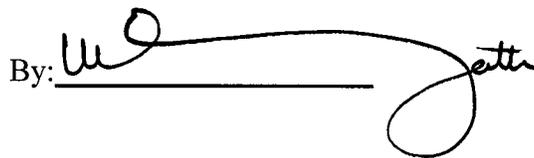
[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

IN WITNESS WHEREOF, the Government of the United States of America and the Government of the Republic of Kenya, each acting through its duly authorized representative, have caused this Agreement to be signed in the English language in their names and delivered as of the day and year written below. In the event that this Grant Agreement is signed in more than one language, the English language version shall govern.

For the Government of the United States of America

For the Government of the Republic of Kenya

By: 

By: 

Ambassador Scott Gration
U.S. Ambassador to Kenya

Date: 3 September 2011

Date: 19/09/2011

Witnessed:

Witnessed:

By: 

By: 

Camille Richardson
Senior Commercial Officer

Bitange Ndiriro
P. S. Information and Communication

Annex I -- Terms of Reference

Annex II – Mandatory Clauses

Annex I

Terms of Reference

National Cybersecurity Master Plan Technical Assistance

Task 1 – Review Regulatory, Policy and Legal Framework

The Contractor shall perform a review of regulations, policy, and law related to cybersecurity in Kenya. This review shall include any regulations which are required to implement and enforce a national cybersecurity master plan in Kenya. The Contractor's review shall cover national, regional (e.g. East African Community), and international policies and laws. After the review, the Contractor shall identify, and discuss with the Grantee, any policy and/or legal gaps in Kenyan Law and regulations that have been identified as part of this review effort. This effort shall provide the groundwork for developing the first deliverable, the *Cybersecurity Policy and Legal Framework*.

The Contractor shall develop a *Cybersecurity Policy and Legal Framework*, which shall provide guidance to the Government of Kenya (GoK) regarding the laws, regulations and policies which may need to be amended, updated, or introduced in order to implement the Project. The Contractor shall develop drafts of proposed regulations, policies and laws for any matters and issues which are not addressed by existing regulations, policies and laws. The *Cybersecurity Policy and Legal Framework* shall address, at minimum, international cybersecurity cooperation, cyber crime, privacy and e-signature. As part of the *Cybersecurity Policy and Legal Framework*, the Contractor shall develop and include a cybersecurity policy which mandates and describes the responsibilities of the GoK agencies and the private sector to secure their critical cyber assets and protect citizens'/clients' data.

Throughout the course of the TA, the Contractor shall continue to monitor any changes in regulations, laws, and institutions that may impact this Project. The Contractor shall also take these regulations, laws, and institutions into account while carrying out Tasks 2-13 below.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Cybersecurity Policy and Legal Framework* that contains all information collected, work performed and analysis provided under Task 1.

Task 2 – Conduct a Cybersecurity Assessment and Gap Analysis

The Contractor shall perform a cybersecurity assessment for the GoK. The Contractor's assessment shall include the identification and documentation of cyber assets that are essential to the reliable operation of critical GoK functions. Cyber assets are those assets that, if destroyed, degraded or rendered unavailable, would affect the reliability or operability of the GoK. At a minimum, these cyber assets shall include network elements, servers, applications and data.

The Contractor shall develop a *GoK Critical Cyber Assets Baseline*, which shall provide the GoK with a listing and corresponding detailed information of the GoK's cyber assets that the Contractor classifies as critical. The *GoK Critical Cyber Assets Baseline* shall include, at a minimum, operational procedures, network topology and/or similar diagrams, data storage locations, equipment layouts of critical cyber assets, disaster recovery plans, incident response plans, and security configuration information.

After identifying the critical cyber assets, the Contractor shall assess GoK's current security vulnerabilities and any applied security measures, and develop a security assessment and gap analysis. This *security assessment and gap analysis* shall provide the GoK with detailed descriptions of any information security gaps in terms of procedures, systems, technology, people and governance that currently exist within the GoK. The *GoK Security Assessment and Gap Analysis* shall also provide the GoK with an evaluation of GoK's current information security posture in comparison with industry best practices and relevant security standards.

Deliverable: The Contractor shall prepare and deliver to the Grantee two reports entitled *GoK Critical Cyber Assets Baseline* and *GoK Security Assessment and Gap Analysis* that contain all information collected, work performed and analysis provided under Task 2.

Task 3 – Develop Information Security Management Procedures

The Contractor shall develop *Information Security Management Procedures* which shall provide the GoK with the minimum set of administrative, technical, and physical safeguards that need to be implemented by the GoK in order to adequately protect its cyber assets and sensitive data. The purpose of these procedures is to implement the applicable cyber security policies identified in Task 1 and to ensure that GoK's agencies and organizations are in compliance with relevant laws, regulations, and mandated standards regarding data privacy, security, and the protection of cyber assets. In addition, the Contractor shall base these procedures on international information security standards and National Institute of Standards and Technology special publications on the subject, as well as best practices. At a minimum, the Contractor shall include the following procedures:

- Access control procedures for managing access to protected critical cyber assets' information;
- Change control and configuration management processes for controlling the addition, modification, or replacement of critical cyber asset hardware and/or software and documenting all of the related changes, and;
- Other security management controls such as security patch management, security status monitoring, and account management.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *GoK Information Security Management Procedures* that contains all information collected, work performed and analysis provided under Task 3.

Task 4 – Develop Cybersecurity Architecture and Design

The Contractor shall develop the *Cybersecurity Architecture and Design* for the GoK, which shall identify the required cybersecurity systems to protect the cyber assets identified in Task 2. The Contractor shall develop the cybersecurity architecture, which shall detail the complete cybersecurity solution and systems, ensuring the security of e-government applications and business information at every point in the architecture. The Contractor shall also document how the cybersecurity architecture and systems will be incorporated and instituted into the existing information system architecture of the GoK. The Contractor's *Cybersecurity Architecture and Design* shall be aligned with the strategies and objectives of the GoK, taking into consideration the importance of data sharing and the provision of online services to citizens and businesses, whilst ensuring the privacy of citizen's sensitive information.

The Contractor shall also develop technical specifications for all of the cybersecurity systems that will need to be procured and deployed across the GoK's networks, servers, data centers, and applications. These systems shall be based on the latest advances in cybersecurity, including proven industry-wide and open standards, and shall also ensure interoperability. At minimum, the Contractor shall design these technical specifications to ensure that the GoK's cybersecurity systems shall provide the following:

- Threat management to address threats to systems such as viruses, Trojans, worms, malicious hackers, force majeure (e.g. war, fire, flood, earthquake, or any other event beyond the reasonable control of the Grantee), and intentional and unintentional system misuse by insiders or outsiders. At a minimum, threat management tools and processes shall include: security monitoring, web application firewalls, security incident management processes, security event management system, incident response planning processes, cryptography, and forensic analysis process and tools;
- Vulnerability management, which includes the set of processes and technologies for discovering, reporting, and mitigating known vulnerabilities. The vulnerabilities may reside at any system layer – database, operating system, servers, and so on. At a minimum, vulnerability management tools include specialized tools to probe for known vulnerabilities;
- Network security, which includes the design and operations for security mechanisms for the network, such as network firewalls and network intrusion detection devices;
- Host security, which is concerned with access control on the servers and workstations. Systems such as host intrusion detection systems need to be deployed to identify host anomalies and security events;
- Application security, which deals with protecting the code and services running on the system, who is connecting to them, and what is the output from the programs, and;
- Data security, which deals with securing access to data and its use.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Cybersecurity Architecture and Design* that contains all information collected, work performed and analysis provided under Task 4.

Task 5 – Develop Identity and Access Management (Trusted Cyber Identities) Requirements

The Contractor shall evaluate, and analyze any existing access management processes, and systems in place within the GoK. The Contractor shall also develop a gap analysis and an identity and access management (IAM) strategy, requirements and high-level design to address these gaps. The IAM solution shall address IAM's four main components, namely: authentication, authorization, user management and central user repository. The goal is to provide the appropriate access to the appropriate people, while allowing efficient and effective management of directory services, user provisioning, web access management, and enterprise single sign-on. At a minimum, the Contractor shall propose a solution that has the capability to:

- Centralize the access request, approval, and management processes;
- Facilitate the use of credentials for authentication, digital signatures, and encryption;
- Enable GoK to implement role-based user provisioning by linking users' access based on assigned business roles/functions;
- Allow for the access rights of managed users to be quickly audited across the GoK, and;
- Enable the provisioning and de-provisioning of new users and accounts across the GoK in timely manner.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Identity and Access Management Requirements* that contains all information collected, work performed and analysis provided under Task 5.

Task 6 – Develop Cybersecurity Organizational Structure and Governance

The Contractor shall evaluate and recommend various organizations, within the GoK, that should be responsible to oversee the implementation of the Project and its various components. The Contractor shall also evaluate these various organizations' roles and responsibilities and propose any changes required to implement the Project. The Contractor's analysis shall include the following organizations: the Ministry of Information and Communications (MoIC), the Kenya ICT Board, Communications Commission of Kenya (CCK), Computer Emergency Readiness Team (CERT), Computer Security Incident Response Team (CSIRT), information security offices of the various government agencies and any other structures or organizations needed to implement the Project.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Cybersecurity Governance Framework* that contains all information collected, work performed and analysis provided under Task 6.

Task 7 –Develop a Cybersecurity Capacity Building and Training Plan

The Contactor shall identify different roles and responsibilities for each cybersecurity personnel at the government agencies in the GoK, and identify these in a *Cybersecurity Personnel - Roles and Responsibilities* document. In this document, the Contractor shall provide the GoK with detailed information about the roles and responsibilities of GoK personnel in regards to cybersecurity.

The Contractor shall then develop a *Training and Capacity Building Plan*, which shall recommend mechanisms to ensure that cybersecurity personnel qualifications are kept current, and that cybersecurity personnel are continually trained to be aware of the latest technology, threats and advances in cybersecurity. The Contractor's plan shall also include the evaluation of the establishment of a cybersecurity center of excellence in Kenya. The Contractor shall not be responsible for the performance of the actual training, nor for the establishment of a cybersecurity center of excellence.

Deliverable: The Contractor shall prepare and deliver to the Grantee two reports entitled *Cybersecurity Personnel - Roles and Responsibilities* and *Cybersecurity Personnel - Training and Capacity Building Plan* that contain all information collected, work performed and analysis provided under Task 7.

Task 8 – Develop a Cybersecurity Implementation and Procurement Plan

Based on the output of Task 4 and Task 5, the Contractor shall develop a *Cybersecurity Implementation and Procurement Plan*, which shall outline all the subsequent steps that the Grantee will need to take in order to implement the recommendations of the TA. To this end, the Contractor shall also take into consideration the findings of Task 1 through Task 7, and shall identify and recommend well-defined implementation phases and a timeline in order to implement the cybersecurity architecture, identified in Task 4, and the identity and access control system identified in Task 5. The Contractor's *Implementation and Procurement Plan* shall also include budgetary requirements for each step included in the plan.

Additionally the Contractor shall develop detailed *Cybersecurity Procurement Documents*, which shall provide the Grantee with descriptions, performance requirements, evaluation criteria, budgets, detailed procurement specifications and draft tender documents for all tasks/phases of the cybersecurity implementation plan that will be implemented during the first two years of the plan.

The procurement documents, which shall be developed by the Contractor, shall not focus solely on the lowest price of the equipment and services, but rather on the overall best value for the GoK. This analysis shall include the consideration of the total cost of ownership (ie, life cycle costing), reliability, scalability, quality, interoperability and conformance to international standards. The Contractor's procurement documents shall avoid proprietary and non-interoperable systems which would cause the GoK to be restricted to the same vendor for any of its future procurements. The Contractor shall develop well-defined evaluation criteria that reflect all of the above considerations in the procurement documents. The procurement documents shall assist the GoK in preparing

the final tenders (Request for Proposals), and procuring the required hardware, software and services to implement the Project.

Deliverable: The Contractor shall prepare and deliver to the Grantee two reports entitled *Cybersecurity Implementation and Procurement Plan* and *Cybersecurity Procurement Documents* that contain all information collected, work performed and analysis provided under Task 8.

Task 9 – Develop a Cybersecurity Awareness Campaign and Deliver Workshops

The Contractor shall develop, organize, and deliver a cybersecurity awareness campaign, which shall consist of delivering cybersecurity awareness workshops. The goal of these workshops shall be to introduce GoK participants to the threats and vulnerabilities in the cyber environment, and provide them with a high level overview of the TA's findings and recommendations, as well as cybersecurity best practices.

The Contractor shall conduct the cybersecurity awareness workshops in coordination with the Grantee at the Grantee's facilities (or at another appropriate venue agreed upon by the Contractor and the Grantee, such venue to be provided at the Grantee's cost). The Contractor shall coordinate with the Grantee on the workshop content and provide all workshop participants with an agenda, workbooks, reference materials, and other handouts or presentation materials. The Contractor shall conduct the workshop and maintain workshop records, including the agenda, workbooks, reference materials, any handouts or presentation materials, a list of all workshop participants, and a description of the workshop, for inclusion in the Final Report.

The Contractor shall obtain the Grantee's approval on the content and materials, prior to delivering the workshops.

The Contractor shall conduct the workshops at various government organizations in Kenya, targeting executive managers and various cybersecurity professionals and users. The Contractor shall deliver four (4) of these workshops for approximately 30-40 trainees per workshop. The duration of each workshop shall be approximately four (4) hours.

The Contractor shall also train GoK's qualified personnel, who will be identified by the Grantee, to conduct similar workshops in the future. The Grantee shall be responsible for arranging the workshop space and the list of trainees. The Contractor shall also develop cybersecurity awareness materials, including posters, and hand-outs for these workshops.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Cybersecurity Awareness Campaign Plan and Related Materials* that contains all information collected, work performed and analysis provided under Task 9.

Task 10 – Conduct a Economic and Financial Analysis

The Contractor shall conduct an economic cost-benefit analysis of the Project, including an analysis of competing alternative methods of achieving the same or similar objectives for the Project. The Contractor shall prepare a financial analysis, which shall provide an

estimate of the total cost to implement the Project, and including the growth of the plan to include new users and new applications over a five (5) year timeframe. The Contractor shall also recommend sources of financing and identify which components can be financed from the MoIC budget and which components shall be financed by other GoK ministries, from the Kenya Transparency Communication Infrastructure Project (TCIP) funded by the World Bank, or from other sources.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Economic and Financial Analysis* that contains all information collected, work performed and analysis provided under Task 10.

Task 11 – Analyze Development Impacts

The Contractor shall assess the development impacts associated with the Project and the methodology for measuring those impacts. The Contractor shall include examples of the development impacts that would be expected in Kenya, if the Project is implemented as outlined in the TA. The Contractor shall focus on examples from the categories listed below and shall develop a methodology for assessing these impacts over time. The Contractor shall only list benefits on the categories that are applicable to the Project. The categories to be considered are as follows:

- **Infrastructure:** How the Project will result in improvements to, or increased investment in, infrastructure (both direct and indirect);
- **Human Capacity Building:** Skills development or additional employment that will be generated within the Grantee or within the selected GOK Ministries;
- **Technology Transfer and Productivity Improvement:** Identification of new recommended technologies deployed in conjunction with the Project, and specific technology or knowledge transfer that will take place;
- **Market-Oriented Reform:** Identification of any market-oriented reforms that will be achieved as a result of the Project, which could include improved competition, better market entry to new investment, or more equitable consumer pricing policies; and
- **Other:** Any other development benefits of the Project, including any spin-off or demonstration effects.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Analysis of Development Impacts* that contains all information collected, work performed and analysis provided under Task 11.

Task 12 – Identify U.S. Sources of Supply

The Contractor shall conduct an assessment of the availability of potential U.S. sources of supply for implementation of the TA recommendations. U.S. sources of supply shall include U.S. providers of all the different categories of goods and services required for implementation of the Project. For each source identified, the Contractor shall include: company name, point of contact, address, telephone, e-mail, and fax numbers and relevant goods and services provided. As part of this research, the Contractor shall

contact at least twenty relevant U.S. companies regarding the TA, and compile a list of those companies that express interest in participating in the Project.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Assessment of U.S. Sources of Supply* that contains all information collected, work performed and analysis provided under Task 12.

Task 13 - Final Report

The Contractor shall prepare and deliver to the Grantee a substantive and comprehensive draft final report of all work performed pursuant to these Terms of Reference (“Draft Final Report”). After the Grantee has reviewed the Draft Final Report, the Contractor shall conduct a final report meeting with the Grantee at the Grantee’s facilities or at another appropriate venue agreed upon by the Contractor and the Grantee, such venue to be provided at the Grantee’s cost. The Grantee shall identify appropriate personnel and other relevant stakeholders to participate in the final report meeting.

During the final report meeting, the Contractor shall: review all work performed under these Terms of Reference; present the findings and recommendations from the Draft Final Report, and; gather feedback from the Grantee on the Draft Final Report and Grantee requests for changes to the Draft Final Report, if any.

For the final report meeting, the Contractor shall: coordinate with the Grantee on appropriate meeting content; prepare an agenda, handouts, and presentation materials, as needed, for all meeting attendees; conduct the meeting and facilitate the discussion; draft a report of the meeting and distribute the meeting report to meeting attendees, and other relevant parties, and; maintain meeting records, including the agenda, any handouts and presentation materials, a list of all meeting participants, and the meeting report, for inclusion in the Final Report.

The Contractor shall prepare and deliver to the Grantee and USTDA a substantive and comprehensive final report of all work performed under these Terms of Reference (“Final Report”). The Final Report shall be organized according to the above tasks, and shall include all deliverables under these Terms of Reference, including all training materials, and documents that have been provided to the Grantee. The Final Report shall also contain an Executive Summary in addition to the other required deliverables, and shall be in accordance with Clause I of Annex II of the Grant Agreement. The Contractor will provide the Grantee with 6 copies of the final report on CD-ROM. The Contractor shall prepare and deliver the Final Report to USTDA in the manner set forth in Clause I of Annex II hereof.

Notes:

- 1. The Contractor is responsible for compliance with U.S. export licensing requirements, if applicable, in the performance of the Terms of Reference.**

- 2. The Contractor and the Grantee shall be careful to ensure that the public version of the Final Report contains no security or confidential information.**
- 3. The Grantee and USTDA shall have an irrevocable, worldwide, royalty-free, non-exclusive right to use and distribute the Final Report and all work product that is developed under these Terms of Reference.**

Annex II

USTDA Mandatory Contract Clauses

A. USTDA Mandatory Clauses Controlling

The parties to this contract acknowledge that this contract is funded in whole or in part by the U.S. Trade and Development Agency ("USTDA") under the Grant Agreement between the Government of the United States of America acting through USTDA and the Government of the Republic of Kenya, acting through the Ministry of Information and Communications ("Client"), dated _____ ("Grant Agreement"). The Client has selected _____ ("Contractor") to perform the Technical Assistance ("TA") for the National Cybersecurity Master Plan project ("Project") in Kenya ("Host Country"). Notwithstanding any other provisions of this contract, the following USTDA mandatory contract clauses shall govern. All subcontracts entered into by Contractor funded or partially funded with USTDA Grant funds shall include these USTDA mandatory contract clauses, except for clauses B(1), G, H, I, and J. In addition, in the event of any inconsistency between the Grant Agreement and any contract or subcontract thereunder, the Grant Agreement shall be controlling.

B. USTDA as Financier

(1) USTDA Approval of Contract

All contracts funded under the Grant Agreement, and any amendments thereto, including assignments and changes in the Terms of Reference, must be approved by USTDA in writing in order to be effective with respect to the expenditure of USTDA Grant funds. USTDA will not authorize the disbursement of USTDA Grant funds until the contract has been formally approved by USTDA or until the contract conforms to modifications required by USTDA during the contract review process.

(2) USTDA Not a Party to the Contract

It is understood by the parties that USTDA has reserved certain rights such as, but not limited to, the right to approve the terms of this contract and amendments thereto, including assignments, the selection of all contractors, the Terms of Reference, the Final Report, and any and all documents related to any contract funded under the Grant Agreement. The parties hereto further understand and agree that USTDA, in reserving any or all of the foregoing approval rights, has acted solely as a financing entity to assure the proper use of United States Government funds, and that any decision by USTDA to exercise or refrain from exercising these approval rights shall be made as a financier in the course of financing the TA and shall not be construed as making USTDA a party to the contract. The parties hereto understand and agree that USTDA may, from time to time, exercise the foregoing approval rights, or discuss matters related to these rights and the Project with the parties to the contract or any subcontract, jointly or separately, without thereby incurring any responsibility or

liability to such parties. Any approval or failure to approve by USTDA shall not bar the Client or USTDA from asserting any right they might have against the Contractor, or relieve the Contractor of any liability which the Contractor might otherwise have to the Client or USTDA.

C. Nationality, Source and Origin

Except as USTDA may otherwise agree, the following provisions shall govern the delivery of goods and services funded by USTDA under the Grant Agreement: (a) for professional services, the Contractor must be either a U.S. firm or U.S. individual; (b) the Contractor may use U.S. subcontractors without limitation, but the use of subcontractors from Host Country may not exceed twenty percent (20%) of the USTDA Grant amount and may only be used for specific services from the Terms of Reference identified in the subcontract; (c) employees of U.S. Contractor or U.S. subcontractor firms responsible for professional services shall be U.S. citizens or non-U.S. citizens lawfully admitted for permanent residence in the U.S.; (d) goods purchased for performance of the TA and associated delivery services (e.g., international transportation and insurance) must have their nationality, source and origin in the United States; and (e) goods and services incidental to TA support (e.g., local lodging, food, and transportation) in Host Country are not subject to the above restrictions. USTDA will make available further details concerning these provisions upon request.

D. Recordkeeping and Audit

The Contractor and subcontractors funded under the Grant Agreement shall maintain, in accordance with generally accepted accounting procedures, books, records, and other documents, sufficient to reflect properly all transactions under or in connection with the contract. These books, records, and other documents shall clearly identify and track the use and expenditure of USTDA funds, separately from other funding sources. Such books, records, and documents shall be maintained during the contract term and for a period of three (3) years after final disbursement by USTDA. The Contractor and subcontractors shall afford USTDA, or its authorized representatives, the opportunity at reasonable times for inspection and audit of such books, records, and other documentation.

E. U.S. Carriers

(1) Air

Transportation by air of persons or property funded under the Grant Agreement shall be on U.S. flag carriers in accordance with the Fly America Act, 49 U.S.C. 40118, to the extent service by such carriers is available, as provided under applicable U.S. Government regulations.

(2) Marine

Transportation by sea of property funded under the Grant Agreement shall be on U.S. carriers in accordance with U.S. cargo preference law.

F. Workman's Compensation Insurance

The Contractor shall provide adequate Workman's Compensation Insurance coverage for work performed under this Contract.

G. Reporting Requirements

The Contractor shall advise USTDA by letter as to the status of the Project on March 1st annually for a period of two (2) years after completion of the TA. In addition, if at any time the Contractor receives follow-on work from the Client, the Contractor shall so notify USTDA and designate the Contractor's contact point including name, telephone, and fax number. Since this information may be made publicly available by USTDA, any information which is confidential shall be designated as such by the Contractor and provided separately to USTDA. USTDA will maintain the confidentiality of such information in accordance with applicable law.

H. Disbursement Procedures

(1) USTDA Approval of Contract

Disbursement of Grant funds will be made only after USTDA approval of this contract. To make this review in a timely fashion, USTDA must receive from either the Client or the Contractor a photocopy of an English language version of a signed contract or a final negotiated draft version to the attention of the General Counsel's office at USTDA's address listed in Clause M below.

(2) Payment Schedule Requirements

A payment schedule for disbursement of Grant funds to the Contractor shall be included in this Contract. Such payment schedule must conform to the following USTDA requirements: (1) up to twenty percent (20%) of the total USTDA Grant amount may be used as a mobilization payment; (2) all other payments, with the exception of the final payment, shall be based upon contract performance milestones; and (3) the final payment may be no less than fifteen percent (15%) of the total USTDA Grant amount, payable upon receipt by USTDA of an approved Final Report in accordance with the specifications and quantities set forth in Clause I below. Invoicing procedures for all payments are described below.

(3) Contractor Invoice Requirements

USTDA will make all disbursements of USTDA Grant funds directly to the Contractor. The Contractor must provide USTDA with an ACH Vendor Enrollment Form (available from USTDA) with the first invoice. The Client shall request disbursement of funds by

USTDA to the Contractor for performance of the contract by submitting the following to USTDA:

(a) Contractor's Invoice

The Contractor's invoice shall include reference to an item listed in the Contract payment schedule, the requested payment amount, and an appropriate certification by the Contractor, as follows:

(i) For a mobilization payment (if any):

"As a condition for this mobilization payment, the Contractor certifies that it will perform all work in accordance with the terms of its Contract with the Client. To the extent that the Contractor does not comply with the terms and conditions of the Contract, including the USTDA mandatory provisions contained therein, it will, upon USTDA's request, make an appropriate refund to USTDA. "

(ii) For contract performance milestone payments:

"The Contractor has performed the work described in this invoice in accordance with the terms of its contract with the Client and is entitled to payment thereunder. To the extent the Contractor has not complied with the terms and conditions of the Contract, including the USTDA mandatory provisions contained therein, it will, upon USTDA's request, make an appropriate refund to USTDA."

(iii) For final payment:

"The Contractor has performed the work described in this invoice in accordance with the terms of its contract with the Client and is entitled to payment thereunder. Specifically, the Contractor has submitted the Final Report to the Client, as required by the Contract, and received the Client's approval of the Final Report. To the extent the Contractor has not complied with the terms and conditions of the Contract, including the USTDA mandatory provisions contained therein, it will, upon USTDA's request, make an appropriate refund to USTDA."

(b) Client's Approval of the Contractor's Invoice

(i) The invoice for a mobilization payment must be approved in writing by the Client.

(ii) For contract performance milestone payments, the following certification by the Client must be provided on the invoice or separately:

"The services for which disbursement is requested by the Contractor have been performed satisfactorily, in accordance with applicable Contract provisions and the terms and conditions of the USTDA Grant Agreement."

(iii) For final payment, the following certification by the Client must be provided on the invoice or separately:

"The services for which disbursement is requested by the Contractor have been performed satisfactorily, in accordance with applicable Contract provisions and terms and conditions of the USTDA Grant Agreement. The Final Report submitted by the Contractor has been reviewed and approved by the Client. "

(c) USTDA Address for Disbursement Requests

Requests for disbursement shall be submitted by courier or mail to the attention of the Finance Department at USTDA's address listed in Clause M below.

(4) Termination

In the event that the Contract is terminated prior to completion, the Contractor will be eligible, subject to USTDA approval, for reasonable and documented costs which have been incurred in performing the Terms of Reference prior to termination, as well as reasonable wind down expenses. Reimbursement for such costs shall not exceed the total amount of undisbursed Grant funds. Likewise, in the event of such termination, USTDA is entitled to receive from the Contractor all USTDA Grant funds previously disbursed to the Contractor (including but not limited to mobilization payments) which exceed the reasonable and documented costs incurred in performing the Terms of Reference prior to termination.

I. USTDA Final Report

(1) Definition

"Final Report" shall mean the Final Report described in the attached Annex I Terms of Reference or, if no such "Final Report" is described therein, "Final Report" shall mean a substantive and comprehensive report of work performed in accordance with the attached Annex I Terms of Reference, including any documents delivered to the Client.

(2) Final Report Submission Requirements

The Contractor shall provide the following to USTDA:

- (a) One (1) complete version of the Final Report for USTDA's records. This version shall have been approved by the Client in writing and must be in the English language. It is the responsibility of the Contractor to ensure that confidential information, if any, contained in this version be clearly marked. USTDA will maintain the confidentiality of such information in accordance with applicable law.

and

(b) One (1) copy of the Final Report suitable for public distribution ("Public Version"). The Public Version shall have been approved by the Client in writing and must be in the English language. As this version will be available for public distribution, it must not contain any confidential information. If the report in (a) above contains no confidential information, it may be used as the Public Version. In any event, the Public Version must be informative and contain sufficient Project detail to be useful to prospective equipment and service providers.

and

(c) Two (2) CD-ROMs, each containing a complete copy of the Public Version of the Final Report. The electronic files on the CD-ROMs shall be submitted in a commonly accessible read-only format. As these CD-ROMs will be available for public distribution, they must not contain any confidential information. It is the responsibility of the Contractor to ensure that no confidential information is contained on the CD-ROMs.

The Contractor shall also provide one (1) copy of the Public Version of the Final Report to the Foreign Commercial Service Officer or the Economic Section of the U.S. Embassy in Host Country for informational purposes.

(3) Final Report Presentation

All Final Reports submitted to USTDA must be paginated and include the following:

(a) The front cover of every Final Report shall contain the name of the Client, the name of the Contractor who prepared the report, a report title, USTDA's logo, USTDA's mailing and delivery addresses. If the complete version of the Final Report contains confidential information, the Contractor shall be responsible for labeling the front cover of that version of the Final Report with the term "Confidential Version." The Contractor shall be responsible for labeling the front cover of the Public Version of the Final Report with the term "Public Version." The front cover of every Final Report shall also contain the following disclaimer:

"This report was funded by the U.S. Trade and Development Agency (USTDA), an agency of the U. S. Government. The opinions, findings, conclusions or recommendations expressed in this document are those of the author(s) and do not necessarily represent the official position or policies of USTDA. USTDA makes no representation about, nor does it accept responsibility for, the accuracy or completeness of the information contained in this report."

(b) The inside front cover of every Final Report shall contain USTDA's logo, USTDA's mailing and delivery addresses, and USTDA's mission statement.

Camera-ready copy of USTDA Final Report specifications will be available from USTDA upon request.

(c) The Contractor shall affix to the front of the CD-ROM a label identifying the Host Country, USTDA Activity Number, the name of the Client, the name of the Contractor who prepared the report, a report title, and the following language:

“The Contractor certifies that this CD-ROM contains the Public Version of the Final Report and that all contents are suitable for public distribution.”

(d) The Contractor and any subcontractors that perform work pursuant to the Grant Agreement must be clearly identified in the Final Report. Business name, point of contact, address, telephone and fax numbers shall be included for Contractor and each subcontractor.

(e) The Final Report, while aiming at optimum specifications and characteristics for the Project, shall identify the availability of prospective U.S. sources of supply. Business name, point of contact, address, telephone and fax numbers shall be included for each commercial source.

(f) The Final Report shall be accompanied by a letter or other notation by the Client which states that the Client approves the Final Report. A certification by the Client to this effect provided on or with the invoice for final payment will meet this requirement.

J. Modifications

All changes, modifications, assignments or amendments to this contract, including the appendices, shall be made only by written agreement by the parties hereto, subject to written USTDA approval.

K. TA Schedule

(1) TA Completion Date

The completion date for the TA, which is September 20, 2013, is the date by which the parties estimate that the TA will have been completed.

(2) Time Limitation on Disbursement of USTDA Grant Funds

Except as USTDA may otherwise agree, (a) no USTDA funds may be disbursed under this contract for goods and services which are provided prior to the Effective Date of the Grant Agreement; and (b) all funds made available under the Grant Agreement must be disbursed within four (4) years from the Effective Date of the Grant Agreement.

L. Business Practices

The Contractor agrees not to pay, promise to pay, or authorize the payment of any money or anything of value, directly or indirectly, to any person (whether a governmental official or private individual) for the purpose of illegally or improperly inducing anyone to take any action favorable to any party in connection with the TA. The Client agrees not to receive any such payment. The Contractor and the Client agree that each will require that any agent or representative hired to represent them in connection with the TA will comply with this paragraph and all laws which apply to activities and obligations of each party under this Contract, including but not limited to those laws and obligations dealing with improper payments as described above.

M. USTDA Address and Fiscal Data

Any communication with USTDA regarding this Contract shall be sent to the following address and include the fiscal data listed below:

U.S. Trade and Development Agency
1000 Wilson Boulevard, Suite 1600
Arlington, Virginia 22209-3901
USA

Phone: (703) 875-4357
Fax: (703) 875-4009

Appropriation No.: 11 11/12 1001
Activity No.: 2011-11027A
Reservation No.: 2011278
Grant No.: GH201111278

N. Definitions

All capitalized terms not otherwise defined herein shall have the meaning set forth in the Grant Agreement.

O. Taxes

USTDA funds provided under the Grant Agreement shall not be used to pay any taxes, tariffs, duties, fees or other levies imposed under laws in effect in Host Country. Neither the Client nor the Contractor will seek reimbursement from USTDA for such taxes, tariffs, duties, fees or other levies.

ANNEX 5

Terms of Reference

National Cybersecurity Master Plan Technical Assistance

Task 1 – Review Regulatory, Policy and Legal Framework

The Contractor shall perform a review of regulations, policy, and law related to cybersecurity in Kenya. This review shall include any regulations which are required to implement and enforce a national cybersecurity master plan in Kenya. The Contractor's review shall cover national, regional (e.g. East African Community), and international policies and laws. After the review, the Contractor shall identify, and discuss with the Grantee, any policy and/or legal gaps in Kenyan Law and regulations that have been identified as part of this review effort. This effort shall provide the groundwork for developing the first deliverable, the *Cybersecurity Policy and Legal Framework*.

The Contractor shall develop a *Cybersecurity Policy and Legal Framework*, which shall provide guidance to the Government of Kenya (GoK) regarding the laws, regulations and policies which may need to be amended, updated, or introduced in order to implement the Project. The Contractor shall develop drafts of proposed regulations, policies and laws for any matters and issues which are not addressed by existing regulations, policies and laws. The *Cybersecurity Policy and Legal Framework* shall address, at minimum, international cybersecurity cooperation, cyber crime, privacy and e-signature. As part of the *Cybersecurity Policy and Legal Framework*, the Contractor shall develop and include a cybersecurity policy which mandates and describes the responsibilities of the GoK agencies and the private sector to secure their critical cyber assets and protect citizens'/clients' data.

Throughout the course of the TA, the Contractor shall continue to monitor any changes in regulations, laws, and institutions that may impact this Project. The Contractor shall also take these regulations, laws, and institutions into account while carrying out Tasks 2-13 below.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Cybersecurity Policy and Legal Framework* that contains all information collected, work performed and analysis provided under Task 1.

Task 2 – Conduct a Cybersecurity Assessment and Gap Analysis

The Contractor shall perform a cybersecurity assessment for the GoK. The Contractor's assessment shall include the identification and documentation of cyber assets that are essential to the reliable operation of critical GoK functions. Cyber assets are those assets that, if destroyed, degraded or rendered unavailable, would affect the reliability or operability of the GoK. At a minimum, these cyber assets shall include network elements, servers, applications and data.

The Contractor shall develop a *GoK Critical Cyber Assets Baseline*, which shall provide the GoK with a listing and corresponding detailed information of the GoK's cyber assets that the Contractor classifies as critical. The *GoK Critical Cyber Assets Baseline* shall include, at a minimum, operational procedures, network topology and/or similar diagrams, data storage

locations, equipment layouts of critical cyber assets, disaster recovery plans, incident response plans, and security configuration information.

After identifying the critical cyber assets, the Contractor shall assess GoK's current security vulnerabilities and any applied security measures, and develop a security assessment and gap analysis. This *security assessment and gap analysis* shall provide the GoK with detailed descriptions of any information security gaps in terms of procedures, systems, technology, people and governance that currently exist within the GoK. The *GoK Security Assessment and Gap Analysis* shall also provide the GoK with an evaluation of GoK's current information security posture in comparison with industry best practices and relevant security standards.

Deliverable: The Contractor shall prepare and deliver to the Grantee two reports entitled *GoK Critical Cyber Assets Baseline* and *GoK Security Assessment and Gap Analysis* that contain all information collected, work performed and analysis provided under Task 2.

Task 3 – Develop Information Security Management Procedures

The Contractor shall develop *Information Security Management Procedures* which shall provide the GoK with the minimum set of administrative, technical, and physical safeguards that need to be implemented by the GoK in order to adequately protect its cyber assets and sensitive data. The purpose of these procedures is to implement the applicable cyber security policies identified in Task 1 and to ensure that GoK's agencies and organizations are in compliance with relevant laws, regulations, and mandated standards regarding data privacy, security, and the protection of cyber assets. In addition, the Contractor shall base these procedures on international information security standards and National Institute of Standards and Technology special publications on the subject, as well as best practices. At a minimum, the Contractor shall include the following procedures:

- Access control procedures for managing access to protected critical cyber assets' information;
- Change control and configuration management processes for controlling the addition, modification, or replacement of critical cyber asset hardware and/or software and documenting all of the related changes, and;
- Other security management controls such as security patch management, security status monitoring, and account management.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *GoK Information Security Management Procedures* that contains all information collected, work performed and analysis provided under Task 3.

Task 4 – Develop Cybersecurity Architecture and Design

The Contractor shall develop the *Cybersecurity Architecture and Design* for the GoK, which shall identify the required cybersecurity systems to protect the cyber assets identified in Task 2. The Contractor shall develop the cybersecurity architecture, which shall detail the complete cybersecurity solution and systems, ensuring the security of e-government applications and business information at every point in the architecture. The Contractor shall also document how

the cybersecurity architecture and systems will be incorporated and instituted into the existing information system architecture of the GoK. The Contractor's *Cybersecurity Architecture and Design* shall be aligned with the strategies and objectives of the GoK, taking into consideration the importance of data sharing and the provision of online services to citizens and businesses, whilst ensuring the privacy of citizen's sensitive information.

The Contractor shall also develop technical specifications for all of the cybersecurity systems that will need to be procured and deployed across the GoK's networks, servers, data centers, and applications. These systems shall be based on the latest advances in cybersecurity, including proven industry-wide and open standards, and shall also ensure interoperability. At minimum, the Contractor shall design these technical specifications to ensure that the GoK's cybersecurity systems shall provide the following:

- Threat management to address threats to systems such as viruses, Trojans, worms, malicious hackers, force majeure (e.g. war, fire, flood, earthquake, or any other event beyond the reasonable control of the Grantee), and intentional and unintentional system misuse by insiders or outsiders. At a minimum, threat management tools and processes shall include: security monitoring, web application firewalls, security incident management processes, security event management system, incident response planning processes, cryptography, and forensic analysis process and tools;
- Vulnerability management, which includes the set of processes and technologies for discovering, reporting, and mitigating known vulnerabilities. The vulnerabilities may reside at any system layer – database, operating system, servers, and so on. At a minimum, vulnerability management tools include specialized tools to probe for known vulnerabilities;
- Network security, which includes the design and operations for security mechanisms for the network, such as network firewalls and network intrusion detection devices;
- Host security, which is concerned with access control on the servers and workstations. Systems such as host intrusion detection systems need to be deployed to identify host anomalies and security events;
- Application security, which deals with protecting the code and services running on the system, who is connecting to them, and what is the output from the programs, and;
- Data security, which deals with securing access to data and its use.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Cybersecurity Architecture and Design* that contains all information collected, work performed and analysis provided under Task 4.

Task 5 – Develop Identity and Access Management (Trusted Cyber Identities) Requirements

The Contractor shall evaluate, and analyze any existing access management processes, and systems in place within the GoK. The Contractor shall also develop a gap analysis and an identity and access management (IAM) strategy, requirements and high-level design to address these gaps. The IAM solution shall address IAM's four main components, namely: authentication, authorization, user management and central user repository. The goal is to provide the appropriate access to the appropriate people, while allowing efficient and effective

management of directory services, user provisioning, web access management, and enterprise single sign-on. At a minimum, the Contractor shall propose a solution that has the capability to:

- Centralize the access request, approval, and management processes;
- Facilitate the use of credentials for authentication, digital signatures, and encryption;
- Enable GoK to implement role-based user provisioning by linking users' access based on assigned business roles/functions;
- Allow for the access rights of managed users to be quickly audited across the GoK, and;
- Enable the provisioning and de-provisioning of new users and accounts across the GoK in timely manner.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Identity and Access Management Requirements* that contains all information collected, work performed and analysis provided under Task 5.

Task 6 – Develop Cybersecurity Organizational Structure and Governance

The Contractor shall evaluate and recommend various organizations, within the GoK, that should be responsible to oversee the implementation of the Project and its various components. The Contractor shall also evaluate these various organizations' roles and responsibilities and propose any changes required to implement the Project. The Contractor's analysis shall include the following organizations: the Ministry of Information and Communications (MoIC), the Kenya ICT Board, Communications Commission of Kenya (CCK), Computer Emergency Readiness Team (CERT), Computer Security Incident Response Team (CSIRT), information security offices of the various government agencies and any other structures or organizations needed to implement the Project.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Cybersecurity Governance Framework* that contains all information collected, work performed and analysis provided under Task 6.

Task 7 –Develop a Cybersecurity Capacity Building and Training Plan

The Contractor shall identify different roles and responsibilities for each cybersecurity personnel at the government agencies in the GoK, and identify these in a *Cybersecurity Personnel - Roles and Responsibilities* document. In this document, the Contractor shall provide the GoK with detailed information about the roles and responsibilities of GoK personnel in regards to cybersecurity.

The Contractor shall then develop a *Training and Capacity Building Plan*, which shall recommend mechanisms to ensure that cybersecurity personnel qualifications are kept current, and that cybersecurity personnel are continually trained to be aware of the latest technology, threats and advances in cybersecurity. The Contractor's plan shall also include the evaluation of the establishment of a cybersecurity center of excellence in Kenya. The Contractor shall not be responsible for the performance of the actual training, nor for the establishment of a cybersecurity center of excellence.

Deliverable: The Contractor shall prepare and deliver to the Grantee two reports entitled *Cybersecurity Personnel - Roles and Responsibilities* and *Cybersecurity Personnel - Training and Capacity Building Plan* that contain all information collected, work performed and analysis provided under Task 7.

Task 8 – Develop a Cybersecurity Implementation and Procurement Plan

Based on the output of Task 4 and Task 5, the Contractor shall develop a *Cybersecurity Implementation and Procurement Plan*, which shall outline all the subsequent steps that the Grantee will need to take in order to implement the recommendations of the TA. To this end, the Contractor shall also take into consideration the findings of Task 1 through Task 7, and shall identify and recommend well-defined implementation phases and a timeline in order to implement the cybersecurity architecture, identified in Task 4, and the identity and access control system identified in Task 5. The Contractor's *Implementation and Procurement Plan* shall also include budgetary requirements for each step included in the plan.

Additionally the Contractor shall develop detailed *Cybersecurity Procurement Documents*, which shall provide the Grantee with descriptions, performance requirements, evaluation criteria, budgets, detailed procurement specifications and draft tender documents for all tasks/phases of the cybersecurity implementation plan that will be implemented during the first two years of the plan.

The procurement documents, which shall be developed by the Contractor, shall not focus solely on the lowest price of the equipment and services, but rather on the overall best value for the GoK. This analysis shall include the consideration of the total cost of ownership (ie, life cycle costing), reliability, scalability, quality, interoperability and conformance to international standards. The Contractor's procurement documents shall avoid proprietary and non-interoperable systems which would cause the GoK to be restricted to the same vendor for any of its future procurements. The Contractor shall develop well-defined evaluation criteria that reflect all of the above considerations in the procurement documents. The procurement documents shall assist the GoK in preparing the final tenders (Request for Proposals), and procuring the required hardware, software and services to implement the Project.

Deliverable: The Contractor shall prepare and deliver to the Grantee two reports entitled *Cybersecurity Implementation and Procurement Plan* and *Cybersecurity Procurement Documents* that contain all information collected, work performed and analysis provided under Task 8.

Task 9 – Develop a Cybersecurity Awareness Campaign and Deliver Workshops

The Contractor shall develop, organize, and deliver a cybersecurity awareness campaign, which shall consist of delivering cybersecurity awareness workshops. The goal of these workshops shall be to introduce GoK participants to the threats and vulnerabilities in the cyber environment, and provide them with a high level overview of the TA's findings and recommendations, as well as cybersecurity best practices.

The Contractor shall conduct the cybersecurity awareness workshops in coordination with the Grantee at the Grantee's facilities (or at another appropriate venue agreed upon by the Contractor

and the Grantee, such venue to be provided at the Grantee's cost). The Contractor shall coordinate with the Grantee on the workshop content and provide all workshop participants with an agenda, workbooks, reference materials, and other handouts or presentation materials. The Contractor shall conduct the workshop and maintain workshop records, including the agenda, workbooks, reference materials, any handouts or presentation materials, a list of all workshop participants, and a description of the workshop, for inclusion in the Final Report.

The Contractor shall obtain the Grantee's approval on the content and materials, prior to delivering the workshops.

The Contractor shall conduct the workshops at various government organizations in Kenya, targeting executive managers and various cybersecurity professionals and users. The Contractor shall deliver four (4) of these workshops for approximately 30-40 trainees per workshop. The duration of each workshop shall be approximately four (4) hours.

The Contractor shall also train GoK's qualified personnel, who will be identified by the Grantee, to conduct similar workshops in the future. The Grantee shall be responsible for arranging the workshop space and the list of trainees. The Contractor shall also develop cybersecurity awareness materials, including posters, and hand-outs for these workshops.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Cybersecurity Awareness Campaign Plan and Related Materials* that contains all information collected, work performed and analysis provided under Task 9.

Task 10 – Conduct a Economic and Financial Analysis

The Contractor shall conduct an economic cost-benefit analysis of the Project, including an analysis of competing alternative methods of achieving the same or similar objectives for the Project. The Contractor shall prepare a financial analysis, which shall provide an estimate of the total cost to implement the Project, and including the growth of the plan to include new users and new applications over a five (5) year timeframe. The Contractor shall also recommend sources of financing and identify which components can be financed from the MoIC budget and which components shall be financed by other GoK ministries, from the Kenya Transparency Communication Infrastructure Project (TCIP) funded by the World Bank, or from other sources.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Economic and Financial Analysis* that contains all information collected, work performed and analysis provided under Task 10.

Task 11 – Analyze Development Impacts

The Contractor shall assess the development impacts associated with the Project and the methodology for measuring those impacts. The Contractor shall include examples of the development impacts that would be expected in Kenya, if the Project is implemented as outlined in the TA. The Contractor shall focus on examples from the categories listed below and shall develop a methodology for assessing these impacts over time. The Contractor shall only list benefits on the categories that are applicable to the Project. The categories to be considered are as follows:

- **Infrastructure:** How the Project will result in improvements to, or increased investment in, infrastructure (both direct and indirect);
- **Human Capacity Building:** Skills development or additional employment that will be generated within the Grantee or within the selected GOK Ministries;
- **Technology Transfer and Productivity Improvement:** Identification of new recommended technologies deployed in conjunction with the Project, and specific technology or knowledge transfer that will take place;
- **Market-Oriented Reform:** Identification of any market-oriented reforms that will be achieved as a result of the Project, which could include improved competition, better market entry to new investment, or more equitable consumer pricing policies; and
- **Other:** Any other development benefits of the Project, including any spin-off or demonstration effects.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Analysis of Development Impacts* that contains all information collected, work performed and analysis provided under Task 11.

Task 12 – Identify U.S. Sources of Supply

The Contractor shall conduct an assessment of the availability of potential U.S. sources of supply for implementation of the TA recommendations. U.S. sources of supply shall include U.S. providers of all the different categories of goods and services required for implementation of the Project. For each source identified, the Contractor shall include: company name, point of contact, address, telephone, e-mail, and fax numbers and relevant goods and services provided. As part of this research, the Contractor shall contact at least twenty relevant U.S. companies regarding the TA, and compile a list of those companies that express interest in participating in the Project.

Deliverable: The Contractor shall prepare and deliver to the Grantee a report entitled *Assessment of U.S. Sources of Supply* that contains all information collected, work performed and analysis provided under Task 12.

Task 13 - Final Report

The Contractor shall prepare and deliver to the Grantee a substantive and comprehensive draft final report of all work performed pursuant to these Terms of Reference (“Draft Final Report”). After the Grantee has reviewed the Draft Final Report, the Contractor shall conduct a final report meeting with the Grantee at the Grantee’s facilities or at another appropriate venue agreed upon by the Contractor and the Grantee, such venue to be provided at the Grantee’s cost. The Grantee shall identify appropriate personnel and other relevant stakeholders to participate in the final report meeting.

During the final report meeting, the Contractor shall: review all work performed under these Terms of Reference; present the findings and recommendations from the Draft Final Report, and; gather feedback from the Grantee on the Draft Final Report and Grantee requests for changes to the Draft Final Report, if any.

For the final report meeting, the Contractor shall: coordinate with the Grantee on appropriate meeting content; prepare an agenda, handouts, and presentation materials, as needed, for all meeting attendees; conduct the meeting and facilitate the discussion; draft a report of the meeting and distribute the meeting report to meeting attendees, and other relevant parties, and; maintain meeting records, including the agenda, any handouts and presentation materials, a list of all meeting participants, and the meeting report, for inclusion in the Final Report.

The Contractor shall prepare and deliver to the Grantee and USTDA a substantive and comprehensive final report of all work performed under these Terms of Reference ("Final Report"). The Final Report shall be organized according to the above tasks, and shall include all deliverables under these Terms of Reference, including all training materials, and documents that have been provided to the Grantee. The Final Report shall also contain an Executive Summary in addition to the other required deliverables, and shall be in accordance with Clause I of Annex II of the Grant Agreement. The Contractor will provide the Grantee with 6 copies of the final report on CD-ROM. The Contractor shall prepare and deliver the Final Report to USTDA in the manner set forth in Clause I of Annex II hereof.

Notes:

- 1. The Contractor is responsible for compliance with U.S. export licensing requirements, if applicable, in the performance of the Terms of Reference.**
- 2. The Contractor and the Grantee shall be careful to ensure that the public version of the Final Report contains no security or confidential information.**
- 3. The Grantee and USTDA shall have an irrevocable, worldwide, royalty-free, non-exclusive right to use and distribute the Final Report and all work product that is developed under these Terms of Reference.**

ANNEX 6

COMPANY INFORMATION

A. Company Profile

Provide the information listed below relative to the Offeror's firm. If the Offeror is proposing to subcontract some of the proposed work to another firm(s), the information requested in sections E and F below must be provided for each subcontractor.

1. Name of firm and business address (street address only), including telephone and fax numbers:

2. Year established (include predecessor companies and year(s) established, if appropriate).

3. Type of ownership (e.g. public, private or closely held).

4. If private or closely held company, provide list of shareholders and the percentage of their ownership.

5. List of directors and principal officers (President, Chief Executive Officer, Vice-President(s), Secretary and Treasurer; provide full names including first, middle and last). Please place an asterisk (*) next to the names of those principal officers who will be involved in the Technical Assistance.

6. If Offeror is a subsidiary, indicate if Offeror is a wholly-owned or partially-owned subsidiary. Provide the information requested in items 1 through 5 above for the Offeror's parent(s).

7. Project Manager's name, address, telephone number, e-mail address and fax number .

B. Offeror's Authorized Negotiator

Provide name, title, address, telephone number, e-mail address and fax number of the Offeror's authorized negotiator. The person cited shall be empowered to make binding commitments for the Offeror and its subcontractors, if any.

C. Negotiation Prerequisites

1. Discuss any current or anticipated commitments which may impact the ability of the Offeror or its subcontractors to complete the Technical Assistance as proposed and reflect such impact within the project schedule.
2. Identify any specific information which is needed from the Grantee before commencing contract negotiations.

D. Offeror's Representations

Please provide exceptions and/or explanations in the event that any of the following representations cannot be made:

1. Offeror is a corporation [*insert applicable type of entity if not a corporation*] duly organized, validly existing and in good standing under the laws of the State of _____ . The Offeror has all the requisite corporate power and authority to conduct its business as presently conducted, to submit this proposal, and if selected, to execute and deliver a contract to the Grantee for the performance of the Technical Assistance. The Offeror is not debarred, suspended, or to the best of its knowledge or belief, proposed for debarment, or ineligible for the award of contracts by any federal or state governmental agency or authority.

2. The Offeror has included, with this proposal, a certified copy of its Articles of Incorporation, and a certificate of good standing issued within one month of the date of its proposal by the State of _____. The Offeror commits to notify USTDA and the Grantee if they become aware of any change in their status in the state in which they are incorporated. USTDA retains the right to request an updated certificate of good standing.
3. Neither the Offeror nor any of its principal officers have, within the three-year period preceding this RFP, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a federal, state or local government contract or subcontract; violation of federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating federal or state criminal tax laws, or receiving stolen property.
4. Neither the Offeror, nor any of its principal officers, is presently indicted for, or otherwise criminally or civilly charged with, commission of any of the offenses enumerated in paragraph 3 above.
5. There are no federal or state tax liens pending against the assets, property or business of the Offeror. The Offeror, has not, within the three-year period preceding this RFP, been notified of any delinquent federal or state taxes in an amount that exceeds \$3,000 for which the liability remains unsatisfied. Taxes are considered delinquent if (a) the tax liability has been fully determined, with no pending administrative or judicial appeals; and (b) a taxpayer has failed to pay the tax liability when full payment is due and required.
6. The Offeror has not commenced a voluntary case or other proceeding seeking liquidation, reorganization or other relief with respect to itself or its debts under any bankruptcy, insolvency or other similar law. The Offeror has not had filed against it an involuntary petition under any bankruptcy, insolvency or similar law.

The selected Offeror shall notify the Grantee and USTDA if any of the representations included in its proposal are no longer true and correct at the time of its entry into a contract with the Grantee.

Signed: _____
(Authorized Representative)

Print Name: _____

Title: _____

Date: _____

Subcontractor Profile

1. Name of firm and business address (street address only), including telephone and fax numbers.

2. Year established (include predecessor companies and year(s) established, if appropriate).

E. Subcontractor's Representations

If any of the following representations cannot be made, or if there are exceptions, the subcontractor must provide an explanation.

1. Subcontractor is a corporation *[insert applicable type of entity if not a corporation]* duly organized, validly existing and in good standing under the laws of the State of _____ . The subcontractor has all the requisite corporate power and authority to conduct its business as presently conducted, to participate in this proposal, and if the Offeror is selected, to execute and deliver a subcontract to the Offeror for the performance of the Technical Assistance and to perform the Technical Assistance. The subcontractor is not debarred, suspended, or to the best of its knowledge or belief, proposed for debarment or ineligible for the award of contracts by any federal or state governmental agency or authority.

2. Neither the subcontractor nor any of its principal officers have, within the three-year period preceding this RFP, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a federal, state or local government contract or subcontract; violation of federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating federal or state criminal tax laws, or receiving stolen property.

3. Neither the subcontractor, nor any of its principal officers, is presently indicted for, or otherwise criminally or civilly charged with, commission of any of the offenses enumerated in paragraph 2 above.
4. There are no federal or state tax liens pending against the assets, property or business of the subcontractor. The subcontractor, has not, within the three-year period preceding this RFP, been notified of any delinquent federal or state taxes in an amount that exceeds \$3,000 for which the liability remains unsatisfied. Taxes are considered delinquent if (a) the tax liability has been fully determined, with no pending administrative or judicial appeals; and (b) a taxpayer has failed to pay the tax liability when full payment is due and required.
5. The subcontractor has not commenced a voluntary case or other proceeding seeking liquidation, reorganization or other relief with respect to itself or its debts under any bankruptcy, insolvency or other similar law. The subcontractor has not had filed against it an involuntary petition under any bankruptcy, insolvency or similar law.

The selected subcontractor shall notify the Offeror, Grantee and USTDA if any of the representations included in this proposal are no longer true and correct at the time of the Offeror's entry into a contract with the Grantee.

Signed: _____
(Authorized Representative)

Print Name: _____

Title: _____

Date: _____