GUAM POWER AUTHORITY
ATURIDÅT ILEKTRESEDÅT GUÅHAN
P.O.BOX 2977 • HAGÅTÑA, GUAM U.S.A. 96932-2977

May 12, 2023

AMENDMENT NO.: VII

TO

INVITATION FOR MULTI-STEP BID NO.: GPA-012-23

FOR

RENEWABLE ENERGY RESOURCE ACQUISITION PHASE IV

Prospective Bidders are hereby notified of the following:

INCLUSIONS:

1. ***REMOVE*** Pages 12b and 13b of 263 and ***REPLACE*** with Pages 12c and 13c of 263 (see attached).

   To include **Cut-Off Date for Receipt of Questions Relative to Bid Amendment No.: VII ONLY** to the bid milestone:

   Under, **Volume I, Commercial Terms and Conditions,** Item **1. Introduction,**

   Changes to the **Table 1: Bid Milestone** as follows:

	Bid Milestones	From Date	To Date
*	**Bid Announcement**	12/01/2022	08/18/2023
	Submit Questions	12/01/2022	02/07/2023
	Cut-Off Date for Receipt of Questions	**02/07/2023 4:00 P.M. CHamoru Standard Time; (CHST)**	
*	**Cut-Off Date for Receipt of Questions Relative to Bid Amendment No. VII Only**	**05/30/2023 4:00 P.M. CHamoru Standard Time; (CHST)**	

*	GPA Review and Answer Questions		02/08/2023	06/23/2023
*	Bidders Prepare Technical Proposals (Unpriced)		06/24/2023	08/18/2023
*	**Cut-Off Date for Receipt of Technical Proposals (Unpriced)**		**08/18/2023 2:00 P.M. CHamoru Standard Time; (CHST)**	
*	Office of Attorney General Approval ***(Note: Delay due to new procurement review requirement per Office of the Attorney General)**		**08/21/2023**	**08/25/2023**
*	**EVALUATION**	Technical Proposal Evaluation	08/28/2023	09/08/2023
*	**Step One:**	Notification of Qualified Bidders	09/11/2023	09/15/2023
*	**EVALUATION Step Two:**	**Cut-Off Date for Receipt of Priced Proposals**	**11/06/2023 2:00 P.M. CHamoru Standard Time; (CHST)**	
*		Opening of Price Proposals (Public Opening)	**11/07/2023 2:00 P.M. CHamoru Standard Time; (CHST)**	
*		Office of Attorney General Approval ***(Note: Delay due to new procurement review requirement per Office of the Attorney General)**	11/08/2023	11/15/2023
*		Evaluation of Price Proposal	11/27/2023	12/01/2023
*		Notification of Successful Bidder(s)	12/04/2023	12/07/2023
	System Integration Study		TBD	TBD
	Contract Finalization		TBD	TBD

	Contract Approval & Recommendation to Award	TBD	TBD
	Public Utilities Commission Review	TBD	TBD
*	Office of Attorney General Approval ***(Note: Delay due to new procurement review requirement per Office of the Attorney General)**	TBD	TBD
	Contract Signing	TBD	

2. ***REMOVE*** Page 107 of 263 and ***REPLACE*** with Page 107a of 263 (see attached).

   Under, **Volume II: Technical Qualification Proposal Requirements,** to include the following:

   * **g. Control System Software**

   GPA has three battery energy storage systems incorporated into its power system at Hagatna, Talofofo, and KEPCO Mangilao Solar Power Plant. They all use inverter-battery controls from PXiSE Energy Solutions. GPA has partnered up with PXiSE on two grant proposals awaiting decision from the United States Government:

   - Integration of Autonomous Grid Controller to Support High Penetration of Renewable Energy on Guam's Electric Grid
   - System Wide nFLISR: An Autonomous and Dynamic Network-wide Fault Location, Isolation and Service Restoration System with Active Control

   Both grant projects would require integration with all BESS inverters for the purpose of centralizing control of all BESS to provide grid services to GPA's power system. This amendment requires all Phase IV Bidders integrate and use the PXiSE control systems as part of their proposal. GPA based this decision on:

   - Reduction of technical risk of integration with systems to be developed under the above grant projects
   - Reduction of risk due to Intellectual Property complexities that may result from separate control system vendors and PXiSE
   - Cybersecurity

3. ***REMOVE*** Page 108 of 263 and ***REPLACE*** *with 108a and 108a.1 of 263 (see attached)***:**

   Under, **Volume II: Technical Qualification Proposal Requirements,** to include the following:

   * **2.2.6. Compliance with Trade Agreements Act**

All GPA purchases of computer, network, communications, and industrial control systems shall comply with the Trade Agreements Act.

In Force Procurement Policy (CRS-0156): All GPA purchases of computer, network, communications, and industrial control systems must adhere to the TAA (Trade Agreements Act) and comply with the GPA Policy Directive on System & Service Acquisition in Appendix P.

Vendors must check and GPA Procurement staff and evaluators verify against 3 sources: country list, vender list and confirmation letter from vendor before ordering equipment and/or components.

a. Check against Country List - Sanctions List Search (treas.gov)
b. Check against vendors against the https://sanctionssearch.ofac.treas.gov/
c. Venders must send GPA a confirmation letter of adherence of not using components before ordering parts.
d. Vendor must check, verify, and report to GPA that the deliverables shipped to GPA comply with TAA at loading and unloading dock.
e. Vendor must provide GPA with their documented quality assurance and change controls process used to determine compliance with TAA.

If there are components used from non-TAA or proscribed countries, the vendor must provide a letter to GPA identifying these components and the country of origin, the component function(s), and whether the component has any communication capabilities or has access to communication services such as the local LAN or the Internet.

If there are components used from non-TAA or proscribed countries, the vendor must perform the following at FAT and again at SAT, or as negotiated with GPA:

- Flash the firmware or program the component with a known source firmware inspected and verified by the vendor for possible cybersecurity vulnerabilities.

If there are software modules/subroutines or portions of code that originate from non-TAA compliant or proscribed countries, the vendor must perform the following at FAT and again at SAT, or as negotiated with GPA:

- Re-compile all source code with that has been inspected and verified by the vendor for possible cybersecurity vulnerabilities.

4. ***REMOVE*** Page 197 of 263 and ***REPLACE*** with Page 197a of 263 (see attached)**:**

   Under, **Volume V: Required Forms, APPENDIX A, Proposal Checklists, DOCUMENT RECEIPT CHECKLIST,** include the following to the list of Appendices:

   * Appendix P – Policy Directive on System & Service Acquisition

* 5. ***ADD Page 245a of 263 -*** **Appendix P: Policy Directive on System & Service Acquisition** (see attached).

CHANGES:

1. ***REMOVE*** Page 3c of 263 and ***REPLACE*** with 3d of 263 (see attached).
Under, **INVITATION FOR BID, INSTRUCTION TO BIDDERS,** Paragraph is changed

FROM:
This bid shall be submitted in the form of, **one (1) original, six (6) bound copies of their bid including one completed electronic copy on one disk of the Qualitative Scoring Workbook including all addenda,** if any to the issuing office above no later than **(Time) 2:00 P.M. (Guam CHamoru Standard Time; ChST), Date: July 14, 2023**. **Once completed electronic copy on another disk of the Price Proposal Workbook by the "Cut-off Date for Receipt of Priced Proposals". Bidders are advised to keep a copy of the completed Workbooks and test the electronic copies on disks prior to submitting them to GPA.** Bid submitted after the time and date specified above shall be rejected. See attached General Terms and Conditions and Sealed Bid Solicitation for details.

TO NOW READ:
✱ This bid shall be submitted in the form of, **one (1) original, six (6) bound copies of their bid including one completed electronic copy on one disk of the Qualitative Scoring Workbook including all addenda,** if any to the issuing office above no later than **(Time) 2:00 P.M. (Guam CHamoru Standard Time; ChST), Date: August 18, 2023**. **Once completed electronic copy on another disk of the Price Proposal Workbook by the "Cut-off Date for Receipt of Priced Proposals". Bidders are advised to keep a copy of the completed Workbooks and test the electronic copies on disks prior to submitting them to GPA.** Bid submitted after the time and date specified above shall be rejected. See attached General Terms and Conditions and Sealed Bid Solicitation for details.

2. ***REMOVE*** Page 102a of 263 and ***REPLACE*** with 102b of 263 (see attached).

Under, **Volume II: Technical Qualification Proposal Requirements,** Item **1. Overview, ENERGY AND CAPACITY** paragraph is changed**:**

FROM:

- **ENERGY AND CAPACITY:** The renewable energy resource shall deliver an annual minimum energy (AC) as specified in the Bidder's Qualitative Proposal with a maximum export capacity of 80 MW (AC) at the interconnection point; this may be a combination of several generation units at one or more sites. However, the nameplate capacity that can be installed may be higher than 80 MW, subject to the maximum additional MW capacity that the GPA system can handle as determined by a System Integration Study. The System Integration Study will be completed within 120 days after evaluation of the Price Proposal(s) and initial notification of the most qualified Bidders.

TO NOW READ:

* • **ENERGY AND CAPACITY:** The renewable energy resource shall deliver an annual minimum energy (AC) as specified in the Bidder's Qualitative Proposal with a maximum export capacity of 60 MW (AC) at the interconnection point; this may be a combination of several generation units at one or more sites. However, the nameplate capacity that can be installed may be higher than 60 MW, subject to the maximum additional MW capacity that the GPA system can handle as determined by a System Integration Study. The System Integration Study will be completed within 120 days after evaluation of the Price Proposal(s) and initial notification of the most qualified Bidders. For proposals with an intermittent renewable energy resource coupled with an energy storage system, GPA will allow 60% of the resource to be DC-coupled to the energy storage system with the remaining 40% AC-coupled to the GPA grid. Therefore, 60% of the total project capacity will deliver firm, energy-shifted power from the energy storage system to the GPA grid. The energy storage system shall also provide ramp-rate control for the power delivered from 40% of the total project capacity such that the ramp-rates are kept within 1% per minute at the guaranteed success rate of 95% during the energy production period. However, before or after a GPA curtailment, this rate may be exceeded at the request of the GPA Power System Control Center operators. GPA will not pay for the energy delivered to the GPA grid that did not meet the guaranteed success rate.

3. ***REMOVE*** Page 103 of 263 and ***REPLACE*** with Page 103a of 263 (see attached).
Under, **Volume II: Technical Qualification Proposal Requirements,** Item **ENERGY STORAGE SYSTEM (ESS)** paragraph is changed**:**

FROM:

- **ENERGY STORAGE SYSTEM (ESS):** The renewable energy resource shall be equipped with an energy storage system (ESS) that meets GPA's requirements as described in Section 2.2.2 Acceptable ESS Technologies. The ESS must provide the following functions:
  - o **ENERGY-SHIFTING:** The primary purpose of the ESS shall be for energy-shifting, which is to deliver the energy produced at another time or period of the day.
  - o **RAPID RESERVE:** The additional function of the ESS is to provide rapid reserve in response to under-frequency events. The total energy exported for these events shall be included in the annual minimum energy requirement.

TO NOW READ:

* • **ENERGY STORAGE SYSTEM (ESS):** The renewable energy resource shall be equipped with an energy storage system (ESS) that meets GPA's requirements as described in ***Section 2.2.2 Acceptable ESS Technologies***. The ESS must provide the following primary functions:
    - **ENERGY-SHIFTING:** The primary purpose of the ESS shall be for energy-shifting, which is to deliver the energy produced at another time or period of the day.
    - **RAPID RESERVE:** The additional function of the ESS is to provide rapid reserve in response to under-frequency events. The total energy exported for these events shall be included in the annual minimum energy requirement.
    - **RAMP-RATE CONTROL:** In this mode, the ESS will supply or absorb real power at the point of interconnection in an attempt to control the power output of the renewable energy resource which is AC-coupled to the GPA grid such that the ramp-rate is limited based on the ramp-rate setpoint. Sufficient SOC management control must be provided for optimal ramp-rate control. Manual and remote changes to the ESS ramp-rate setpoint shall also be allowed if needed.

Bidders shall also provide the other grid services in the table below:

Grid Service	Description
Firm Power Dispatch	Provide Dispatchable Renewable Energy
Operating Reserve	Standby Generation Reserve
Fast Frequency Regulation	Rapid injection or absorption of power in response to changes in frequency to maintain system frequency within a tight bandwidth
Rapid Reserve	Respond to fast frequency decay due to trip of large generators on the GPA system by immediate injection of power to the grid to balance generation and demand and prevent underfrequncy load shedding.
Shaping and Firming	Smoothing out intermitency of the renewable resource.
Black Start	Capability to Black Start other Generators over the Transmission System
Grid Forming	Capability to form and supply Microgrids post-natural disaster (i.e., typhoons) or system blackouts.
Energy Shifting	Long Duration Energy Storage System Function
Volt/Var Optimization	Steady state and dynamic management and optimization of Power System Voltages

All other Terms and Conditions in the bid package shall remain unchanged and in full force.

for JOHN M. BENAVENTE, P.E.
General Manager

This bid shall be a Two Step process. Step One will establish a Qualified Bidders List (QBL) based on acceptable submitted non-price Bid information (or Technical Qualification Proposals). Step One is the period from IFB announcement through Notification of Qualified Bidders. Step Two will evaluate the Priced Proposals from the vendors identified on the QBL and which, if any, Qualified Bidder(s) will be awarded a contract(s). Step Two is the period after completion of the Technical Proposal Evaluation and notification of the QBL to the contract award date.

GPA will qualify the Bidders based on their Technical Qualification Proposals and the Qualitative Scoring Workbook. GPA will notify the Bidders selected for the QBL and will proceed with the second step of the bid process to open the sealed bid Priced Proposals of the qualified bidders. GPA will perform a comprehensive evaluation of each bid and select the Bidder(s) with the best bids based on the submitted purchase power price, minimum guarantees, and required technical data.

After the selection of the winning Bidders(s), GPA will conduct system integration studies, at the selected Bidders' expense, to determine system upgrades or improvements required and the associated cost necessary for the selected renewable resource's integration into the GPA transmission system.

If the selected Bidder(s) cannot proceed with the contract, GPA may elect to
1) go to the next best Bidder; or
2) cancel the bid.

Table 1: Bid Milestones indicate the anticipated milestones in the Bid Process.

GPA reserves the right to change the Bid Milestones at its sole discretion. Bidders are encouraged to confirm with GPA any of the scheduled milestones via an official letter to GPA.

Table 1: Bid Milestones

Bid Milestones	From Date	To Date
Bid Announcement	12/01/2022	08/18/2023
Submit Questions	12/01/2022	02/07/2023
Cut-Off Date for Receipt of Questions	**02/07/2023 4:00 P.M. CHamoru Standard Time; (CHST)**	
Cut-Off Date for Receipt of Questions Relative to Bid Amendment No.: VII ONLY	**05/30/2023 4:00 P.M. CHamoru Standard Time; (CHST)**	
GPA Review and Answer Questions	02/08/2023	06/23/2023
Bidders Prepare Technical Proposals (Unpriced)	06/24/2023	08/18/2023

Cut-Off Date for Receipt of Technical Proposals (Unpriced)		**08/18/2023 2:00 P.M. CHamoru Standard Time, (CHST)**	
Office of Attorney General Approval ***(Note: Delay due to new procurement review requirement per Office of the Attorney General)**		**08/21/2023**	**08/25/2023**
EVALUATION Step One:	Technical Proposal Evaluation	08/28/2023	09/08/2023
	Notification of Qualified Bidders	09/11/2023	09/15/2023
EVALUATION Step Two:	**Cut-Off Date for Receipt of Priced Proposals**	**11/06/2023 2:00 P.M. CHamoru Standard Time; (CHST)**	
	Opening of Price Proposals (Public Opening)	**11/07/2023 2:00 P.M. CHamoru Standard Time; (CHST)**	
	Office of Attorney General Approval ***(Note: Delay due to new procurement review requirement per Office of the Attorney General)**	11/08/2023	11/15/2023
	Evaluation of Price Proposal	11/27/2023	12/01/2023
	Notification of Successful Bidder(s)	12/04/2023	12/07/2023
System Integration Study		TBD	TBD
Contract Finalization		TBD	TBD
Contract Approval & Recommendation to Award		TBD	TBD
Public Utilities Commission Review		TBD	TBD
Office of Attorney General Approval ***(Note: Delay due to new procurement review requirement per Office of the Attorney General)**		TBD	TBD
Contract Signing		TBD	

1.1. Invitation for Bid (IFB) Document Organization

Invitation for Bid (IFB) documents are organized into six separate volumes, as follows:

Volume I — Commercial Terms and Conditions

Volume II — Technical Qualification Requirements

Volume III — Draft Renewable Energy Purchase Agreement

Volume IV — Bid Scoring Mechanism

Volume V — Appendices

In addition, the IFB documents include two (2) sets of electronic spreadsheets (MS Excel Workbooks):

- Qualitative Proposal Scoring.xls
- Price Proposal Evaluation.xls

f. SCADA/EMS/SA/AGC Communications Protocol

The ESS shall have the capability to interface with GPA's SCADA, EMS, Substation Automation (SA) and AGC systems over the latest stable release of serial and IP based DNP 3-Secure Authentication communications protocol.

GPA requires the project control system to report each inverter failure or cessation to the GPA SCADA system. The controller will report any alarm that can lead to a system or individual converter cessation or tripping to the GPA SCADA system. The controller will report all delivered power to GPA from the PV system, curtailed power from the PV system, ESS charging power, ESS power, (real and reactive) delivered to GPA, ESS state charge.

Bidder shall provide Bidder's guaranteed success rate according to the size of ESS in the Qualitative Scoring Workbook. The bidder shall also describe the method of calculating and monitoring the success rate in the technical proposal.

* **g. Control System Software**

GPA has three battery energy storage systems incorporated into its power system at Hagatna, Talofofo, and KEPCO Mangilao Solar Power Plant. They all use inverter-battery controls from PXiSE Energy Solutions. GPA has partnered up with PXiSE on two grant proposals awaiting decision from the United States Government:

- Integration of Autonomous Grid Controller to Support High Penetration of Renewable Energy on Guam's Electric Grid
- System Wide nFLISR: An Autonomous and Dynamic Network-wide Fault Location, Isolation and Service Restoration System with Active Control

Both grant projects would require integration with all BESS inverters for the purpose of centralizing control of all BESS to provide grid services to GPA's power system. This amendment requires all Phase IV Bidders integrate and use the PXiSE control systems as part of their proposal. GPA based this decision on:

- Reduction of technical risk of integration with systems to be developed under the above grant projects
- Reduction of risk due to Intellectual Property complexities that may result from separate control system vendors and PXiSE
- Cybersecurity

2.2.3. Proven Technology

The proposed resource technology and key components must have a minimum of one (1) year of operating experience in commercial utility application.

If the proposed technology is a "scale up" of an existing facility, the operational performance data for the smaller plant must be at least 1/10 the proposed plant size or larger.

2.2.4. Use of GPA Facilities

The use of GPA sites or facilities (with the exception of interconnection facilities) will NOT be permitted in this RFP.

2.2.5. Limits on Renewable Energy Purchases

Due to the nature of the generation control system and related response characteristics of the generators on the GPA system, GPA may limit the amount of energy delivered from renewable resources to no more than 30MW (AC) at the interconnection point.

The Bidder shall complete the Energy Projection table in the Technical Bid Form providing its estimated schedule of hourly deliveries of energy for a representative period of time period sufficient for GPA to understand the variability of the expected renewable resource and the impact of total generation costs as part of the Priced Offer evaluations. These estimates must match the annual Minimum Energy Production guarantees discussed further in ***Section 2.3 Project Capacity & Production***.

✱ 2.2.6. Compliance with Trade Agreements Act

All GPA purchases of computer, network, communications, and industrial control systems shall comply with the Trade Agreements Act.

In Force Procurement Policy (CRS-0156): All GPA purchases of computer, network, communications, and industrial control systems must adhere to the TAA (Trade Agreements Act) and comply with the GPA Policy Directive on System & Service Acquisition in Appendix P.

Vendors must check and GPA Procurement staff and evaluators verify against 3 sources: country list, vender list and confirmation letter from vendor before ordering equipment and/or components.

a. Check against Country List - Sanctions List Search (treas.gov)
b. Check against vendors against the https://sanctionssearch.ofac.treas.gov/
c. Venders must send GPA a confirmation letter of adherence of not using components before ordering parts.
d. Vendor must check, verify, and report to GPA that the deliverables shipped to GPA comply with TAA at loading and unloading dock.
e. Vendor must provide GPA with their documented quality assurance and change controls process used to determine compliance with TAA.

If there are components used from non-TAA or proscribed countries, the vendor must provide a letter to GPA identifying these components and the country of origin, the component function(s), and whether the component has any communication capabilities or has access to communication services such as the local LAN or the Internet.

If there are components used from non-TAA or proscribed countries, the vendor must perform the following at FAT and again at SAT, or as negotiated with GPA:

- Flash the firmware or program the component with a known source firmware inspected and verified by the vendor for possible cybersecurity vulnerabilities.

If there are software modules/subroutines or portions of code that originate from non-TAA compliant or proscribed countries, the vendor must perform the following at FAT and again at SAT, or as negotiated with GPA:

- Re-compile all source code with that has been inspected and verified by the vendor for possible cybersecurity vulnerabilities.

2.3. Project Capacity & Production

2.3.1. Minimum and Maximum Project Capacity

The minimum export capacity that a Bidder may offer is 5 MW, and the maximum export capacity shall be 80 MW for each project. This may be the combination of several generation units at one site.

2.3.2. Annual Minimum Guaranteed Production Quantity

The Bidder will provide a guarantee for an Annual Minimum Quantity, in MWh, to be delivered to GPA's system. Subsequent failure to provide this guaranteed Annual Minimum Quantity will subject the Bidder to penalties as described in Renewable Energy Purchase Agreement. The Bidder will also provide the expected minimum (also in MWh) to be delivered each year of the contract period, at a 95% confidence level.

2.4. Delivery

2.4.1. Interconnection

The Bidder will deliver renewable energy to a GPA-determined interconnection point on GPA's 115 kV or 34.5 kV transmission system. GPA will determine the exact location after completion of a detailed interconnection study. The GPA transmission system and primary delivery points are identified in the attached map (See Appendix K). GPA requests that the Bidders identify potential interconnection sites within their submittal.

GPA is recommending the following interconnection requirements. Note that final interconnection agreement will be based on System Integration Study recommendations.

1. An underground loop system in and out of a new substation at the renewable generation facility at transmission level (34.5kV and up) connecting to an existing GPA transmission line. The rerouted transmission line, its associated breakers, and control and protection devices, etc. may require upgrade.

DOCUMENT RECEIPT CHECKLIST

Document Title	Proponent Initial
Volume I Commercial Terms and Conditions	_____
Volume II Technical Qualification Requirements	_____
Volume III Purchase Power Agreement (Draft)	_____
Volume IV Proposal Scoring Mechanism	_____
Volume V Appendices	
APPENDIX A – Proposal Checklist	_____
APPENDIX B – Bid Bond Form and Instructions	_____
APPENDIX C – Ownership & Interest Disclosure Affidavit	_____
APPENDIX D – Non-Collusion Affidavit	_____
APPENDIX E – Local Procurement Preference Application	_____
APPENDIX F – Performance Bond	_____
APPENDIX G – No Gratuities or Kickbacks Affidavit	_____
APPENDIX H – Ethical Standards Affidavit	_____
APPENDIX I – Declaration of Compliance with US DOL's Wage Determination	_____
APPENDIX J – Restriction Against Sex Offenders	_____
APPENDIX K – Electrical System Drawings	_____
APPENDIX L – Required Interconnection Technical Information	_____
APPENDIX M – §3118 (Cost or Pricing Data) & §6101 ((9) Liquidated Damages) of the Guam Procurement Regulations	_____
APPENDIX N – Historical LEAC – Fuel Recovery Rates	_____
APPENDIX O – Potential Utility Solar Sites	_____
* APPENDIX P - Policy Directive on System & Service Acquisition	_____
Qualitative Scoring Workbook.xls	_____
Priced Proposal Workbook.xls	_____
Contiguous Amendment Notifications From Amendment No. 1 through _____	_____
Others:	_____

***APPENDIX P**

Policy Directive on System & Service Acquisition

POLICY DIRECTIVE ON SYSTEM & SERVICE ACQUISITION

System and Networks (SGSN)

PREPARED FOR:	**GUAM POWER AUTHORITY**
EFFECTIVE DATE:	**09/08/2011**
PREPARED BY:	**BLACK & VEATCH**
DOCUMENT NUMBER:	**SA -UTILITIES-1**
VERSION NUMBER:	**1**

©Black & Veatch Holding Company 2011. All rights reserved.

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

Table of Contents

Revision History **5**
1 Introduction **6**
1.1 Purpose 6
1.2 Intended Audience 6
1.3 Scope 6
1.4 Inheritance 6
1.5 Governing Regulation 6
1.6 Review, Update and Approval 7
1.7 Compliance Management 7
2 SDLC Methodology **8**
2.1 Understanding 8
2.2 Purpose and Scope 8
2.3 Audiance 8
2.4 Phases in the SDLC 10
2.4.1 Guam Power Authority' SDLC includes five phases: 11
2.5 Phase 1: initiation 12
2.6 Phase 2: development/acquisition 14
2.7 Phase 3: implementation/assessment 15
2.8 Phase 4: operations/maintenance, and 17
2.9 Phase 5: disposal 20
3 Information System Documentation **21**
4 Software Usage Restrictions **23**
4.1 Inappropriate Use of Assigned SGSN Resources: 23
5 External Information System Services **24**
5.1 Third –party agreements 24
5.2 Monitor Service Provider Performance 25
6 Appendix A **26**
Confidentiality, Integrity and Availability (CIA) 26
6.1 26
7 Approvals **42**

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

LIST OF TABLES

Table 1-1 - Policy Directives Mapped to Cyber Security Manual Policies 7
Table 1-2 - Compliance Management Required Documents 7
Table 2-1 - Key Security Roles and Responsibilities in SDLC 8
Table 2-3 - Key Security Activities Phase 2 14
Table 2-4 - Key Security Activities Phase 3 16
Table 2-5 - Key Security Activities Phase 4 17
Table 6-1 - SGSN Security Control Baseline for CIA 26

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

Revision History

NAME	DATE	REASON FOR CHANGE	VERSION
Black & Veatch	August 20, 2011	Original document	0.01
Black & Veatch	June 1, 2012	Quality Assurance Review	0.02

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

1 Introduction

1.1 PURPOSE

The purpose of this document is to address System and Service Acquisition as described in the Cyber Security Manual.

1.2 INTENDED AUDIENCE

This System & Service Acquisition Directive is directed at Guam Power Authority personnel whom are responsible for hiring, managing and interacting with personnel and contractors.

1.3 SCOPE

The systems in scope for this System & Service Acquisition Directive are as follows:

Initial Phase

- AMI/MDMS/Communications
  - Electric Smart meter (ESM)
- Distribution Automation (DA)
- Distribution Management System (DMS)
- Substation Automation (SA)
- Volt/Var Optimization
- Outage Management System (OMS)
- Load Control Management System (LCMS)
- Mobil Workforce Management (MWM)
- Customer Information System (CIS)
- E-Portal
- Geospatial Information System (GIS)

Future Phase

- Enterprise Asset Management (EAM)
- Demand Response (DR)
- Home Area Network(HAN)

1.4 INHERITANCE

This document is derived as part of Guam Power Authority' Cyber Security Policy. This document inherits all policies and requirements from this document.

1.5 GOVERNING REGULATION

The System & Service Acquisition Directive is derived from the policies contained in the Cyber Security Policy and outlined in the Cyber Security Manual. In order to improve intra-organizational clarity the following table maps the procedure to the approved policies contained in the Cyber Security Manual (CSM).

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

Table 1-1 - Policy Directives Mapped to Cyber Security Manual Policies

POLICY	CSM POLICY	POLICY LANGUAGE
System Development Life Cycle (SDLC)	7.2	A uniform System Development Life-Cycle (SDLC) methodology shall be established and followed to manage all Guam Power Authority SGSNs adequately. The Guam Power Authority best practices maintain a system development life cycle methodology that includes information security considerations and will recommend that appropriate personnel are assigned roles and responsibilities to fulfill the needs of that methodology.

1.6 REVIEW, UPDATE AND APPROVAL

This document shall be reviewed:

- Annually;
- When The Cyber Security Review Committee, as described in the Policy Directive on Governance, mandates an organizational review;
- When the appropriate Senior Manager, as described in the Policy Directive on Governance, mandates an organizational review;

The responsibility for reviewing and updating this document shall lie with the appropriate Senior Manager as designated in the Policy Directive on Governance.

The reviewing and updating of this document must be completed no later than sixty (60) days after any of the conditions above have been met.

Approval of this document shall lie with the appropriate Senior Manager and the Cyber Security Review Committee.

1.7 COMPLIANCE MANAGEMENT

The following documents are required to accurately measure the performance and effectiveness of the cyber security controls listed in this Cyber Security Manual.

Table 1-2 - Compliance Management Required Documents

ID	SECTION	DESCRIPTION	ARTIFACT
CSM-1	7.2	Cyber Security Manual	Methodology (Process) on System Development Life Cycle
CSM-1	7.2	Cyber Security Manual	Documentation of System Documentation Retrieval

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

2 SDLC Methodology

2.1 UNDERSTANDING

Consideration of security in the System Development Life Cycle is essential to implementing and integrating a comprehensive strategy for managing risk for all information technology assets in an organization.

2.2 PURPOSE AND SCOPE

The purpose of this guideline is to provide implementation guidance in building security into Guam Power Authority IT development processes. This should result in more cost-effective, risk-appropriate security control identification, development, and testing. This Methodology focuses on the information security components of the SDLC.

First, the methodology describes the key security roles and responsibilities that are needed in development of most information systems. Second, sufficient information about the SDLC is provided to allow a person who is unfamiliar with the SDLC process to understand the relationship between information security and the SDLC.

2.3 AUDIANCE

This methodology is intended to serve a diverse Guam Power Authority audience of information system and information security professionals including:

- Individuals with information systems and information security management and oversight responsibilities (e.g., chief information officers, senior manager information security officers, and authorizing officials);
- Organization officials having a vested interest in the accomplishment of organizational missions (e.g., mission and business area owners, information owners);
- Individuals with information system development responsibilities (e.g., program and project managers, information system developers);
- Individuals with information security implementation and operational responsibilities (e.g., program and project managers, information system developers); and,
- Individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system security officers).

Table 2-1 - Key Security Roles and Responsibilities in SDLC

ROLES	RESPONSIBILITIES
Authorizing Official (AO)	An AO is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organization operations and assets, individuals, other organizations, and the Nation. To do this, the AO relies primarily on: The completed security plan; The security assessment report; and, The plan of action and milestones for reducing or eliminating information system vulnerabilities.

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

ROLES	RESPONSIBILITIES
Chief Information Officer (CIO)	The CIO is responsible for the organization's information system planning, budgeting, investment, performance, and acquisition. As such, the CIO provides advice and assistance to senior organization personnel in acquiring the most efficient and effective information system to fit the organization's enterprise architecture.
Configuration Management (CM) Manager	The CM manager is responsible for managing the effects of changes or differences in configurations on an information system or network. Thus, the CM manager assists in streamlining change management processes and prevents changes that could detrimentally affect the security posture of a system before they happen.
Contracting Officer	The Contracting Officer is the person who has the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.
Contracting Officer's Technical Representative	The COTR is a qualified employee appointed by the Contracting Officer to act as their technical representative in managing the technical aspects of a contract.
Information System Security Officer	The Information System Security Officer is responsible for ensuring the security of an information system throughout its life cycle.
Information Technology Investment Board (or equivalent)	The Information Technology (IT) Investment Board, or its equivalent, is responsible for managing the CPIC process defined by the Clinger-Cohen Act of 1996 (Section 5).
Legal Advisor/Contract Attorney	The legal advisor is responsible for advising the team on legal issues during the acquisition process.
Privacy Officer	The privacy officer is responsible for ensuring that the services or system being procured meet existing privacy policies regarding protection, dissemination (information sharing and exchange), and information disclosure.
Program Manager / Official (Information Owner)	This person represents business and programmatic interests in the information system during the SDLC process. The program manager plays an essential role in security and is, ideally, intimately aware of functional system requirements.
QA/Test Director	The QA/Test Director is responsible for system test and evaluation, and functions as a resource across a variety of programs by assisting in the development and execution of test plans in conjunction with Program Managers and customers. This person reviews system specifications and determines test needs, and works with Program Managers to plan activities leading up to field test activities.
Senior Information Security Officer (SISO)	The SISO, also known as Chief Information Security Officer, is responsible for promulgating policies on security integration in the SDLC and developing enterprise standards for information security. This individual plays a leading role in introducing an appropriate structured methodology to help identify, evaluate, and minimize information security risks to the organization.
Software Developer	The developer is responsible for programmatic coding regarding applications, software, and Internet/intranet sites, including "secure coding," as well as coordinating and working with the Configuration Management (CM) manager to identify, resolve, and implement controls and other CM issues.

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

ROLES	RESPONSIBILITIES
System Architect	As the overall designer and integrator of the application, the system architect is responsible for creating the overall design architecture and for maintaining the conceptual integrity of the architecture throughout the project life cycle. The System Architect is also responsible for ensuring the quality of technical work products delivered by the project team, including designs, specifications, procedures, and documentation.
System Owner	The system owner is responsible for the procurement, development, integration, modification, operation, and maintenance of an information system.
Other Participants	The list of SDLC roles in an information system development can grow as the complexity increases. It is vital that all development team members work together to ensure that a successful development is achieved. Because information security officials must make critical decisions throughout the development process, they should be included as early as possible in the process. System users may assist in the development by helping the program manager to determine the need, refine the requirements, and inspect and accept the delivered system. Participants may also include personnel who represent IT, configuration management, design and engineering, and facilities groups.

2.4 PHASES IN THE SDLC

Enterprise architecture is a management practice employed by organizations to maximize the effectiveness of mission/business processes and information resources in helping to achieve mission/business success.

Enterprise architecture establishes a clear and unambiguous connection from investments (including information security investments) to measurable performance improvements whether for an entire organization or portion of an organization. Enterprise architecture also provides an opportunity to standardize, consolidate, and optimize information technology assets. These activities ultimately produce information systems that are more transparent and therefore, easier to understand and protect. In addition to establishing a roadmap for more efficient and cost-effective usage of information technology throughout organizations, enterprise architecture provides a common language for discussing risk management issues related to missions, business processes, and performance goals—enabling better coordination and integration of efforts and investments across organizational and business activity boundaries. A well-designed enterprise architecture implemented organization-wide, promotes more efficient, cost-effective, consistent, and interoperable information security capabilities to help organizations better protect missions and business functions—and ultimately more effectively manage risk.

Implementing information security early in the project allows the requirements to mature as needed and in an integrated and cost-effective manner. Engineering security into a product's initiation phase typically costs less than acquiring technologies later that may need to be reconfigured, customized or may provide more or fewer security controls than required. Security should be included during the requirements generation of any project. Designing a solution with consideration for security could substantially reduce the need for additive security controls.

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

The information security architecture describes the security-related aspects of the enterprise architecture that are incorporated into the enterprise architecture definition as an integral part of the architecture development—that is a sub-architecture derived from the enterprise architecture, not a separately defined layer or architecture.

A key component of the enterprise architecture is the embedded information security architecture that provides a roadmap to ensure that mission/business process-driven information security requirements and protection needs are defined and allocated to appropriate organizational information systems and the environments in which those systems operate.

2.4.1 Guam Power Authority' SDLC includes five phases:

2.4.1.1 Initiation

- During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

2.4.1.2 Development/acquisition

- During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed.

2.4.1.3 Implementation/assessment

- After system acceptance testing, the system is installed or fielded.

2.4.1.4 Operations/maintenance

- During this phase, the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events.

2.4.1.5 Disposal

- Activities conducted during this phase ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system, or preserving it in accordance with applicable records management regulations and policies.

Each phase includes a minimum set of security tasks needed to effectively incorporate security in the system development process. Note that phases may continue to be repeated throughout a system's life prior to disposal.

In order to provide clear, concise guidance to the reader, each life cycle phase is described in a section below that has been organized in this manner:

- Provides a brief description of the SDLC phase.
- Identifies general control gates, or established points in the life cycle, when the system will be evaluated and when management will determine whether the project should continue as is, change direction, or be discontinued. Control gates should be flexible and tailored to the specific organization. Control gates are valuable in that they provide the organization with the opportunity to verify that security considerations are being addressed, adequate security is being

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

built in, and identified risks are clearly understood before the system development advances to the next life cycle phase.

Identifies and describes major security activities in each phase. Each activity is then further defined in the following areas:

- Description. The description provides a detailed overview of the activity and highlights specific considerations necessary to address the task.
- Expected Outputs. Common task deliverables and artifacts are listed along with suggestions for forward/backward integration of these work products into the SDLC.
- Synchronization. A feedback loop that provides opportunities to ensure that the SDLC is implemented as a flexible approach that allows for appropriate and consistent communication and the adaptation of tasks and deliverables as the system is developed.
- Interdependencies. This section identifies key interdependencies with other tasks to ensure that security integration activities are not negatively impacted by other IT processes.

2.5 PHASE 1: INITIATION

During this first phase of the development life cycle, security considerations are key to diligent and early integration, thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered. At this point, security is looked at more in terms of business risks with input from the information security office. For example, a GPA may identify a political risk resulting from a prominent website being modified or made unavailable during a critical business period, resulting in decreased trust by citizens.

At the appropriate points in the initiation process, GPA management will:

- Define the security-related roles and responsibilities to be carried out during the SDLC process for the proposed system.
- Identify individuals having information system security roles and responsibilities.
- Specify and make provisions for handling the confidential information regarding the system's security provisions and the confidential functions to implement the security during the SDLC process.
- Define GPA management's need(s) and derive the desired mission functions for the proposed system from the need(s).
- Identify security-related considerations for the proposed system and the system's information in terms of confidentiality, integrity, and availability.

Key security activities for this phase include:

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

Table 2-2 - Key Security Activities Phase 1

TASK	NIST CONTROL	CATEGORY	ARTIFACT
1. Business partner engagement			
2. Document enterprise architecture	PM-7	Enterprise Architecture	
3. Identify/specify applicable policies & laws			
4. Develop C, I, & A objectives	RA-2 PM-9 PM-10 PM-11	Security Categorization Risk Management Strategy Security Authorization Process Mission/Business Process Definition	RA-2 Senior Management Approval of Risk Assessment Results RA-2 Risk Assessment Results PM-10 Designation of Delegate(s) PM-11 Risk Assessment Results
5. Information & Information System Security Categorization	RA-2	Security Categorization	RA-2 Senior Management Approval of Risk Assessment Results RA-2 Risk Assessment Results
6. Procurement specification development	PM-3 SA-3 SA-9	Information Security Resources Life Cycle Support External Information System Services	PM-3 Exceptions to the Capital Planning Requirements SA-3 Proof of Periodic Risk Assessment Result Review SA-3 Records of External Information System Services Compliance Reviews
7. Preliminary risk assessment	RA-3	Risk Assessment	RA-3 Proof of Periodic Risk Assessment Result Review

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

2.6 PHASE 2: DEVELOPMENT/ACQUISITION

This section addresses security considerations unique to the second SDLC phase.

At the appropriate points in the Development and/or Acquisition processes, GPA management will:

- Conduct a risk assessment (RA) of the proposed SGSN in accordance with GPA's approved RA methodology.
- Select the security controls to be put in place for the system.
- Add the necessary security elements to the design of the system.
- Implement the security controls and considerations in the system.
- Add the necessary information about the security controls to GPA's In Scope Systems management's operational documentation (configuration management, incident response, security training, etc.).
- Test the operation of the security controls as part of the system testing process and remediate any issues before authorizing and/or accrediting the system.

Key security activities for this phase include:

Table 2-3 - Key Security Activities Phase 2

TASK	NIST CONTROL	CATEGORY	ARTIFACT
1. Risk Assessment	RA-3	Risk Assessment	RA-3 Proof of Periodic Risk Assessment Result Review
2. Select initial baseline of security controls	RA-2 RA-3 CA-6	Security Categorization Risk Assessment Security Authorization	RA-2 Senior Management Approval of Risk Assessment Results RA-2 Risk Assessment Results RA-3 Proof of Periodic Risk Assessment Result Review CA-6 Senior Manager Authorization of Information Systems and Security Assessment
3. Refinement – security control baseline			
4. Security control design	SA-3 SA-4	Life Cycle Support Acquisitions	SA-3 Proof of Periodic Risk Assessment Result Review SA-3 Records of External Information System Services Compliance Reviews
5. Cost analysis & reporting	SA-2 PM-3	Allocation of Resources Information	SA-2 Planning Business Cases PM-3 Exceptions to the Capital Planning Requirements

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

TASK	NIST CONTROL	CATEGORY	ARTIFACT
		Security Resources	PM-3 Documentation of Capital Planning Business Cases PM-3 Proof of Resource Availability
6. Security planning	PL-2	System Security Plan	PL-2 Approval of System Security Plan PL-2 Review of System Security Plan PL-2 Proof of Update to System Security Plan
7. Unit/integration ST&E	SI-2	Information Output Handling and Retention	SI-2 Documentation of the Assessment of Patches SI-2 Documentation of the Implementation of Patches

2.7 PHASE 3: IMPLEMENTATION/ASSESSMENT

Implementation/Assessment is the third phase of the SDLC. During this phase, the system will be installed and evaluated in the organization's operational environment.

At the appropriate points in the implementation process, GPA management will:

- Create a Security Test and Evaluation plan in accordance with the Security Test and Evaluation Plan, for the security authorization of the system.
- Implement the system's security controls in the system and the production environment.
- Conduct a security assessment for the authorization of the system.
- Review the results of the assessment with the Senior Security Officer or designee. If security issues exist, return the system to the Development phase for redevelopment or record the decision and rationale to authorize the system.
- Update the GPA's Systems Security Plan (Cyber Security Manual) to include the security controls for the system.
- Update the SGSN Plan of Action and Milestones (POA&M) for any unresolved security issues that are authorized to be present when the system is in production.

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

- Issue an official security authorization for the new system.
- Establish a baseline understanding of the existing environment, the decision makers will need to use metrics and the principle of total cost of ownership (TCO) to ensure the most accurate data will be used for decision-making purposes. This data will also set performance targets and cost estimates for service agreements in later phases. GPA shall take the following actions:
- Baseline the existing environment using metrics, gathering and analysis and TCO
- Analyze opportunities and barriers
- Identify options and risks

Key security activities for this phase include:

Table 2-4 - Key Security Activities Phase 3

TASK	NIST CONTROL	CATEGORY	ARTIFACT
1. Product/component inspection	SI-2	Flaw Remediation	SI-2 Documentation of the Assessment of Patches SI-2 Documentation of the Implementation of Patches
2. Security control integration			
3. User/administrative guidance	SA-5 PL-4 PS-6	Security Alerts, Advisories, and Directives Rules of Behavior Access Agreements	SA-5 Vulnerability Assessment Results Analysis SA-5 Vulnerability Remediation Action Plan SA-5 Documentation of System Documentation Retrieval PL-4 Personnel Rules of Behavior for Information Systems PL-4 Signed Acknowledgement of Receipt of Rules of Behavior PS-6 Access Agreements
4. System Security Test & Evaluation (ST&E)	SI-2	Flaw Remediation	SI-2 Documentation of the Assessment of Patches SI-2 Documentation of the Implementation of Patches
5. Security Certification	CA-2 CA-6	Security Assessments	CA-2 Security Assessment Results CA-6 Senior Manager Authorization

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

TASK	NIST CONTROL	CATEGORY	ARTIFACT
		Security Authorization	of Information Systems and Security Assessment
6. Statement of residential			Documentation of Exceptions
7. Security accreditation	CA-2 CA-6	Security Assessments Security Authorization	CA-2 Security Assessment Results CA-6 Senior Manager Authorization of Information Systems and Security Assessment

2.8 PHASE 4: OPERATIONS/MAINTENANCE, AND

Operations and Maintenance is the fourth phase of the SDLC. In this phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. The system is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated. The operational system is periodically assessed to determine how the system can be made more effective, secure, and efficient. Operations continue as long as the system can be effectively adapted to respond to an organization's needs while maintaining an agreed-upon risk level. When necessary modifications or changes are identified, the system may reenter a previous phase of the SDLC.

At the appropriate points in the Operations and Maintenance processes, GPA management will:

- Record maintenance requirements and schedules for the system in accordance with established methods.
- Apply GPA's SGSN management's configuration management practices to the system.
- Apply GPA's management's security monitoring and management practices to the system.

Key security activities for this phase include:

Table 2-5 - Key Security Activities Phase 4

TASK	NIST CONTROL	CATEGORY	ARTIFACT
Continuous auditing	AU-6	Audit Review, Analysis, and Reporting	AU-6 Report on Review of Audit Records
Recertification	CA-2 CA-6	Security Assessments Security Authorization	CA-2 Security Assessment Results CA-6 Senior Manager Authorization of Information Systems and Security Assessment
Reaccreditations	CA-2 CA-6	Security Assessments	CA-2 Security Assessment Results

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

TASK	NIST CONTROL	CATEGORY	ARTIFACT
		Security Authorization	CA-6 Senior Manager Authorization of Information Systems and Security Assessment
Incident handling	IR-1 IR-2 IR-4 IR-5 IR-6 IR-7 IR-8	Incident Response Policy and Procedures Incident Response Training Incident Handling Incident Monitoring Incident Reporting Incident Response Assistance Incident Response Plan	IR-2 Incident Response Training Records IR-2 Incident Response Training Materials IR-4 Post Incident Response Analysis IR-8 Approval of Incident Response Plan IR-8 List of Incident Response Personnel IR-8 Review of Incident Response Plan IR-8 Proof of Revising of Incident Response Plan IR-8 Communique of Incident Response Plan Changes
Auditing	AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-8 AU-9 AU-11 AU-12	Audit and Accountability Policy and Procedures Auditable Events Content of Audit Records Audit Storage Capacity Response to Audit Processing Failures Audit Review, Analysis, and Reporting	AU-2 List of Events System Must be Capable of Auditing AU-4 Approved Audit Storage Capacity Determination AU-6 Report on Review of Audit Records AU-6 Notification and Approval of Report Results to Management AU-12 Audit Records

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

TASK	NIST CONTROL	CATEGORY	ARTIFACT
		Time Stamps Protection of Audit Information Audit Record Retention Audit Generation	
Intrusion detection & monitoring	SC-5 SC-7 SC-20 AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-8 AU-9 AU-11 AU-12	Denial of Service Protection Boundary Protection Secure Name /Address Resolution Service (Authoritative Source) Audit and Accountability Policy and Procedures Auditable Events Content of Audit Records Audit Storage Capacity Response to Audit Processing Failures Audit Review, Analysis, and Reporting	SC-5 List of Specifically Defended Denial of Service Attacks AU-2 List of Events System Must be Capable of Auditing AU-4 Approved Audit Storage Capacity Determination AU-6 Report on Review of Audit Records AU-6 Notification and Approval of Report Results to Management AU-12 Audit Records

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

TASK	NIST CONTROL	CATEGORY	ARTIFACT
		Time Stamps Protection of Audit Information Audit Record Retention Audit Generation	
1. Contingency plan testing (including continuity of operation plan)	CP-3	Information System Connections	CP-3 Recovery Plan Training Materials CP-3 Recovery Plan Training Records
2. Continuous auditing	AU-6	Audit Review, Analysis, and Reporting	AU-6 Report on Review of Audit Records

2.9 PHASE 5: DISPOSAL

Disposal, the final phase in the SDLC, provides for disposal of a system and closeout of any contracts in place. Information security issues associated with information and system disposal should be addressed explicitly. When information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that government resources and assets are protected.

Usually, there is no definitive end to a system. Systems normally evolve or transition to the next generation because of changing requirements or improvements in technology. System security plans should continually evolve with the system. Much of the environmental, management, and operational information should still be relevant and useful in developing the security plan for the follow-on system.

The disposal activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.

At the appropriate points in the Transition and Disposal processes, GPA management will:

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

- Create and execute a Transition plan for the system's functions.
- Create a Disposal plan for the system if applicable.
- Archive any critical information or records for the system.
- Sanitize the system's media in accordance with the Media Protection Directive.
- Dispose of the system's hardware and software in accordance with GPA's management's practices.

GPA shall develop a System Development Life Cycle Methodology sub-directive to describe the chosen approach and its component parts.

Key security activities for this phase include:

Table 2-6 - Key Security Activities Phase 5

TASK	NIST CONTROL	CATEGORY	ARTIFACT
1. Transition planning	SA-3	Life Cycle Support	
2. Component disposal	MP-6	Media Sanitization	MP-6 Proof of Media and Information Sanitization MP-6 Records of the Disposal or Redeployment of Cyber Assets
3. Media sanitization	MP-6	Media Sanitization	MP-6 Proof of Media and Information Sanitization MP-6 Records of the Disposal or Redeployment of Cyber Assets
4. Information Archiving	SI-12	Information Output Handling and Retention	

3 Information System Documentation

GPA shall develop, or caused to be developed, documentation for all SGSN and their constituent components. GPA shall ensure the documentation is available, protected when required, and distributed only to authorized personnel. The administrative and user guides and/or manuals shall include information on configuring, installing, and operating the information system, and for optimizing the system's security features. The guides and/or manuals shall be reviewed periodically, and, if necessary, updated as new vulnerabilities are identified and/or new security controls are added.

GPA management will protect as required, and make available to authorized personnel, administrator and user documentation for the information system that describes:

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

- Secure configuration, installation, and operation of the information system;
- Effective use and maintenance of security features/functions; and
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions and compensating controls for the same.
- User-accessible security features/functions and how to effectively use those security features/functions;
- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
- User responsibilities in maintaining the security of the information and information system.

GPA's will ensure that the documentation:

- Is protected in accordance with the confidentiality level for the applicable system
- Contains sufficient information regarding the functions of the security controls for the in-scope system, components, and services to enable GPA's to perform analysis and testing of the security controls
- Contains sufficient information regarding the design and interaction of the systems, subsystems and implementation details of the security controls for the in-scope system, components, and services to enable GPA to perform analysis and testing of the security controls
- Contains all necessary information (configuration, implementation, administration, operations, maintenance, etc.) to enable the responsible job roles to ensure that the system complies with GPA's applicable security standards
- Contains guidance on the recommended methods of maintaining GPA's security standards when using the system
- Is constructed so as to present the necessary information to the applicable job roles without disclosing information for which a given role does not have security authorization

Where such documentation is unobtainable or unable to be created, GPA will document the attempts to obtain or create the documentation and the reasons for the failure of the effort and retain the records throughout the life cycle of the system.

Implementation Guidance for System Documentation:

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

- Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.
- Maintain an updated list of related system operations and security documentation.
- Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.
- Document the system's configuration, and procedures in support of system access administration and operations.
- Ensure that system documentation describes the functional properties of the security controls implemented within the information system with sufficient detail to facilitate analysis and testing of the controls.

4 Software Usage Restrictions

GPA shall do the following:

- Use software and associated documentation in accordance with contract agreements and copyright laws;
- Employ tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
- Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance or reproduction of copyrighted work.

All software or shareware and associated documentation used on GPA information systems shall be deployed and maintained in accordance with appropriate license agreements and copyright laws. Software associated documentation protected by quantity licenses shall be managed through a tracking system to control copying and distribution. All other uses not specifically authorized by the license agreement shall be prohibited. The use of publicly accessible peer-to-peer file sharing technology shall be controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Only GPA-approved software is to be utilized as specified on the Functional Application Profile (FAP). All applications installed for users must be approved, listed on their GPA Functional Applications Profile (FAP), and handled by IT.

4.1 INAPPROPRIATE USE OF ASSIGNED SGSN RESOURCES:

It is inappropriate to load unauthorized software on a GPA-owned device. The use and copying of software is governed by applicable software license agreements. Generally, copying of software is prohibited or very limited by such license agreements. The installation of software by anyone other than authorized in-scope system or security administrators is prohibited.

All software installations on SGSN must be managed according to the Configuration Management process.

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

All software must be licensed to GPA management or free for commercial use during the period of its use by GPA. GPA's management must possess current documentation of the license for the software.

All software installed on SGSN must be monitored for security issues in accordance with GPA's security monitoring practices. Any issues detected which could feasibly affect the security controls of the system must be corrected in accordance with GPA's patch management practices.

5 External Information System Services

GPA shall:

- Require that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- Define and document government oversight and user roles and responsibilities with regard to external information system services; and
- Monitor security control compliance by external service providers.

All external information system service agreements shall include specific provisions requiring the service provider to comply with GPA policies, standards, and guidelines; and shall be monitored for compliance. GPA shall define the remedies for any loss, disruption, or damage caused by the service provider's failure to comply. Service providers shall be prohibited from outsourcing any system function overseas, unless explicitly authorized, in writing, by the GPA General Manager or his/her designated representatives with concurrence from GPA IT Manager.

For SGSN or functions utilizing third-party services, for the duration of the use of the third-party service, the personnel responsible for the aspect of the in SGSN or function (configuration, administration, operation, etc.) utilizing the third-party service will be responsible for ensuring the compliance of the third party with the security provisions specified in the contract.

5.1 THIRD –PARTY AGREEMENTS

Agreements, regardless of type, should specify the following:

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

- Explicit definitions of both the organization's roles and responsibilities and the service provider's roles and responsibilities (including level of clearance or background investigation needed for staff)
- Description of the service environment, including locations, facility security requirements, and policies, procedures, and standards; and, agreements and licenses
- Defined service levels and service level costs. The service level section of the service agreement may stipulate various service levels for different types of customers or price levels and it may stipulate different service levels for various periods of performance, e.g., year 1 may demand a higher service level than year 2 of the contract
- Defined process regarding how the managers will assess the service provider's compliance with the service level and due date targets, rules, and other terms of the agreement
- Specific remedies (e.g., financial, legal) for noncompliance or harm caused by the service provider
  - Period of performance and/or deliverable due dates
  - Service provider's interface to organization's management
  - GPA 's responsibilities with respect to making information and resources available to service provider
  - Procedures and protections for commingling GPA and service provider data
  - Explicit rules for handling sensitive data.

5.2 MONITOR SERVICE PROVIDER PERFORMANCE

The targets set forth in the service agreement shall be compared with the metrics gathered. Although metrics will provide service-level targets, GPA may use end user evaluations or customer satisfaction level surveys to evaluate performance. The IT security managers shall work with other operational managers (such as customer service managers) to ensure that the service provider is meeting service targets. The IT security managers shall ensure service providers are complying with IT security policy and processes, as well as applicable laws and regulations. IT security managers must ensure during the operations phase that the service provider does not compromise private, confidential, personal, or mission-sensitive data. Compliance reports will help with this effort. The service agreement should have included clauses that specify penalties and/or remedies for noncompliance and management should employ these when the service provider does not perform as the contract dictates.

GPA shall develop an External Information System Services Management Plan sub-directive.

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

6 Appendix A

6.1 CONFIDENTIALITY, INTEGRITY AND AVAILABILITY (CIA)

Table 6-1 - SGSN Security Control Baseline for CIA

SGSN Security Control Baseline for CIA						
CNTL NO.	**SDLC**	**Control Name**	**Priority**	**Confidentiality**	**Integrity**	**Availability**
		Access Control				
AC-1	SDLC	Access Control Policy and Procedures	P1	**X**	**X**	X
AC-2		Account Management	P1	**X**	**X**	
AC-3		Access Enforcement	P1	**X**	**X**	
AC-7		Unsuccessful Login Attempts	P2	**X**	**X**	X
AC-8		System Use Notification	P1	**X**	**X**	
AC-14		Permitted Actions without Identification or Authentication	P1	**X**	**X**	
AC-17		Remote Access	P1	**X**	**X**	
AC-18		Wireless Access	P1	**X**	**X**	
AC-19		Access Control for Mobile Devices	P1	**X**	**X**	
AC-20		Use of External Information Systems	P1	**X**	**X**	
AC-22		Publicly Accessible Content	P2	**X**		
		Awareness and Training				
AT-1	SDLC	Security Awareness and Training Policy and Procedures	P1	**X**	**X**	**X**
AT-2		Security Awareness	P1	**X**	**X**	**X**
AT-3		Security Training	P1	**X**	**X**	**X**
AT-4		Security Training Records	P3	**X**	**X**	**X**
		Audit and Accountability				

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

SGSN Security Control Baseline for CIA						
CNTL NO.	**SDLC**	**Control Name**	**Priority**	**Confidentiality**	**Integrity**	**Availability**
AU-1	SDLC	Audit and Accountability Policy and Procedures	P1	X	X	X
AU-2	SDLC	Auditable Events	P1	X	X	
AU-3	SDLC	Content of Audit Records	P1	X	X	
AU-4	SDLC	Audit Storage Capacity	P1			X
AU-5	SDLC	Response to Audit Processing Failures	P1			X
AU-6	SDLC	Audit Review, Analysis, and Reporting	P1	X	X	
AU-8	SDLC	Time Stamps	P1		X	
AU-9	SDLC	Protection of Audit Information	P1	X	X	
AU-11	SDLC	Audit Record Retention	P3			X
AU-12	SDLC	Audit Generation	P1	X	X	X
		Security Assessment and Authorization				
CA-1	SDLC	Security Assessment and Authorization Policies and Procedures	P1	X	X	X
CA-2	SDLC	Security Assessments	P2	X	X	X
CA-3		Information System Connections	P1	X	X	
CA-5	SDLC	Plan of Action and Milestones	P3	X	X	X
CA-6	SDLC	Security Authorization	P3	X	X	X
		Configuration Management				
CM-1	SDLC	Configuration Management Policy and Procedures	P1	X	X	
CM-2	SDLC	Baseline Configuration	P1		X	
CM-4	SDLC	Security Impact Analysis	P2		X	
CM-6	SDLC	Configuration Settings	P1		X	

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

SGSN Security Control Baseline for CIA						
CNTL NO.	**SDLC**	**Control Name**	**Priority**	**Confidentiality**	**Integrity**	**Availability**
CM-7		Least Functionality	P1	X	X	
CM-8		Information System Component Inventory	P1		X	
		Contingency Planning				
CP-1	SDLC	Contingency Planning Policy and Procedures	P1	X	X	X
CP-2		Contingency Plan	P1			X
CP-3	SDLC	Contingency Training	P2			X
CP-4		Contingency Plan Testing and Exercises	P2			X
CP-9		Information System Backup	P1	X	X	X
CP-10		Information System Recovery and Reconstitution	P1			X
		Identification and Authentication				
IA-1	SDLC	Identification and Authentication Policy and Procedures	P1	X	X	
IA-2		Identification and Authentication (Organizational Users)	P1	X	X	
IA-4		Identifier Management	P1	X	X	
IA-5		Authenticator Management	P1	X	X	
IA-6		Authenticator Feedback	P1	X		
IA-7		Cryptographic Module Authentication	P1	X	X	
IA-8		Identification and Authentication (Non-Organizational Users)	P1	X	X	
		Incident Response				
IR-1	SDLC	Incident Response Policy and Procedures	P1	X	X	X
IR-2	SDLC	Incident Response Training	P2	X	X	X

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

SGSN Security Control Baseline for CIA						
CNTL NO.	**SDLC**	**Control Name**	**Priority**	**Confidentiality**	**Integrity**	**Availability**
IR-4	SDLC	Incident Handling	P1	X	X	X
IR-5	SDLC	Incident Monitoring	P1	X	X	X
IR-6	SDLC	Incident Reporting	P1	X	X	X
IR-7	SDLC	Incident Response Assistance	P3	X	X	X
IR-8	SDLC	Incident Response Plan	P1	X	X	X
		Maintenance				
MA-1	SDLC	System Maintenance Policy and Procedures	P1	X	X	X
MA-2		Controlled Maintenance	P2	X	X	X
MA-4		Non-Local Maintenance	P1		X	
MA-5		Maintenance Personnel	P1	X	X	X
		Media Protection				
MP-1	SDLC	Media Protection Policy and Procedures	P1	X	X	X
MP-2		Media Access	P1	X		
MP-6	SDLC	Media Sanitization	P1	X		
		Physical and Environmental Protection				
PE-1	SDLC	Physical and Environmental Protection Policy and Procedures	P1	X	X	X
PE-2		Physical Access Authorizations	P1	X	X	X
PE-3		Physical Access Control	P1	X	X	X
PE-6		Monitoring Physical Access	P1	X	X	X
PE-7		Visitor Control	P1	X	X	
PE-8		Access Records	P3	X	X	

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

SGSN Security Control Baseline for CIA						
CNTL NO.	**SDLC**	**Control Name**	**Priority**	**Confidentiality**	**Integrity**	**Availability**
PE-12		Emergency Lighting	P1			X
PE-13		Fire Protection	P1			X
PE-14		Temperature and Humidity Controls	P1			X
PE-15		Water Damage Protection	P1			X
PE-16		Delivery and Removal	P1	X		X
		Planning				
PL-1	SDLC	Security Planning Policy and Procedures	P1	X	X	X
PL-2	SDLC	System Security Plan	P1	X	X	X
PL-4	SDLC	Rules of Behavior	P1	X	X	X
		Personnel Security				
PS-1	SDLC	Personnel Security Policy and Procedures	P1	X	X	X
PS-2		Position Categorization	P1	X	X	X
PS-3		Personnel Screening	P1	X	X	
PS-4		Personnel Termination	P2	X	X	X
PS-5		Personnel Transfer	P2	X	X	X
PS-6	SDLC	Access Agreements	P3	X	X	
PS-7		Third-Party Personnel Security	P1	X	X	
PS-8		Personnel Sanctions	P3	X	X	X
		Risk Assessment				
RA-1	SDLC	Risk Assessment Policy and Procedures	P1	X	X	X
RA-2	SDLC	Security Categorization	P1	X	X	X
RA-3	SDLC	Risk Assessment	P1	X	X	X
RA-5		Vulnerability Scanning	P1	X	X	X

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

SGSN Security Control Baseline for CIA						
CNTL NO.	**SDLC**	**Control Name**	**Priority**	**Confidentiality**	**Integrity**	**Availability**
System and Services Acquisition						
SA-1	SDLC	System and Services Acquisition Policy and Procedures	P1	X	X	
SA-2	SDLC	Allocation of Resources	P1		X	
SA-3	SDLC	Life Cycle Support	P1		X	
SA-4	SDLC	Acquisitions	P1		X	
SA-5	SDLC	Information System Documentation	P2		X	
SA-6		Software Usage Restrictions	P1	X	X	
SA-7		User-Installed Software	P1		X	
SA-9	SDLC	External Information System Services	P1		X	
System and Communications Protection						
SC-1	SDLC	System and Communications Protection Policy and Procedures	P1	X	X	X
SC-5	SDLC	Denial of Service Protection	P1			X
SC-7	SDLC	Boundary Protection	P1	X	X	
SC-12		Cryptographic Key Establishment and Management	P1	X	X	
SC-13		Use of Cryptography	P1	X	X	
SC-14		Public Access Protections	P1		X	X
SC-15		Collaborative Computing Devices	P1	X		
SC-20	SDLC	Secure Name /Address Resolution Service (Authoritative Source)	P1		X	
System and Information Integrity						
SI-1	SDLC	System and Information Integrity Policy and Procedures	P1	X	X	X

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

SGSN Security Control Baseline for CIA						
CNTL NO.	**SDLC**	**Control Name**	**Priority**	**Confidentiality**	**Integrity**	**Availability**
SI-2	SDLC	Flaw Remediation	P1		X	
SI-3		Malicious Code Protection	P1		X	
SI-5		Security Alerts, Advisories, and Directives	P1		X	
SI-12	SDLC	Information Output Handling and Retention	P2	X	X	
		Program Management				
PM-1		Information Security Program Plan	P1	X	X	X
PM-2		Senior Information Security Officer	P1	X	X	X
PM-3	SDLC	Information Security Resources	P1	X	X	X
PM-4		Plan of Action and Milestones Process	P1	X	X	X
PM-5		Information System Inventory	P1	X	X	X
PM-6		Information Security Measures of Performance	P1	X	X	X
PM-7	SDLC	Enterprise Architecture	P1	X	X	X
PM-8		Critical Infrastructure Plan	P1	X	X	X
PM-9	SDLC	Risk Management Strategy	P1	X	X	X
PM-10	SDLC	Security Authorization Process	P1	X	X	X
PM-11	SDLC	Mission/Business Process Definition	P1	X	X	X

6.2 CYBERSECURITY ACQUISITION CHECKLIST

Guam Power Authority (GPA) as part of its American Recovery and Reinvestment Act (ARRA) Smart Grid Systems and Networks (SGSN) project followed the Department of Homeland Security: Cyber Security Procurement Language for Control Systems and the Trade Agreements Act (19 U.S.C. & 2501-2581).

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

Cyber Security Procurement Language for Control Systems

The Cyber Security Procurement Language for Control Systems effort was established in March 2006. The results of this endeavor represent the joint effort of the public and private sectors focused on the development of common procurement language for use by all control systems stakeholders. The goal of this document was for federal, state, and local asset owners and regulators to obtain a common control systems security understanding; using these procurement guidelines will help them foster this understanding and lead to integration of security into control systems.

TAA refers to the Trade Agreements Act (19 U.S.C. & 2501-2581).

TAA requires that the U.S. Government acquire products that are produced or undergo a "substantial transformation" within the United States or a designated country.

TAA compliant products make it possible for U.S. government agencies and educational institutions to do business with a USA based company like Trenton Systems. Federal procurement contracts that require TAA compliance include GSA (General Services Administration) Schedule contracts, IDIQ (Indefinite Delivery, Indefinite Quantity) contracts, and most DoD (Department of Defense) contracts.

GPA specifically confirms that the major components that it acquires or purchases, and installed are designed, manufactured, assembled, tested, and supported in the United States from US and international components.

GPA makes every effort including the use of a cybersecurity Acquisition Checklist for the use and acquisition of equipment required to meet and exceed the TAA standards outlined above.

It is GPA'S responsibility to make sure that all products follow the acquisition process and are U.S. made or designated from approved countries. We have a strong set of Internal documented NIST control that we use to confirm the origin of components and parts of our products.

TAA refers to the Trade Agreements Act (19 U.S.C. & 2501-2581).

The vendor response should include at a minimum, but not be limited to, the applicable requirements below:

Cybersecurity Acquisition Checklist		
1.0	GPA Cyber Security Supply Chain Requirements Governing regulation includes: • Department of Homeland Security: Cyber Security Procurement Language for control Systems Sept 2009 • Trade Agreements Act (19 U.S.C. & 2501-2581).	
Department of Homeland Security: Cyber Security Procurement Language for control Systems Sept 2009		
1.1	Security Standard Compliance Full Set of:	Therefore, it is required that the vendor supply chain methodologies, policies, procedures, personnel, products, and services used to design, build, code, configure, manage

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

	GPA Policy GPA (SA) Standard on System and Service Acquisition	data, integrate, test, deploy, implement, and support their GPA solutions, comply with the currently released and applicable security standards including but not limited to NIST SP 800-53 v4 and current NERC CIP 002- CIP-014 standards
1.2	Security Standard Revisions GPA (SA) Standard on System and Service Acquisition Section 4.0	The vendor shall be expected to review new releases and/or updates of subject security standards for applicability to their system solutions implemented at GPA.
1.3	System Resiliency Response – No mapping	The vendor system solutions shall by designed to provide operational resiliency relative to, but not limited to, self-Shealing, fault tolerance, disaster recovery, and alerts of failed resiliency status/events.
1.4	Architecture Resiliency Recommendation	The vendor shall provide technical recommendations to GPA for the design, deployment, and operational implementation within scope of vendor contracted responsibility and control of resilient infrastructure architectures (such as but not limited to offsite Disaster Recovery (DR) implementation) to best support the resiliency of their System products.
1.5	Deployment and Operational Security	The vendor shall provide and apply secure processes, mechanisms, and procedures for the deployment and operational implementation of their System products and services within scope of the vendor contracted responsibility and control such as but not limited to protecting and limiting access to field tools, laptops, digital and non-digital media, and System devices during the initial deployment and recurring operational support phases of the GPA implementation. The vendor shall also ensure any 3rd party entities it contracts to support the execution of its products apply and provide deployment and operational security processes, mechanisms, and procedures equivalent to, or greater than their own respective measures. For deployment and operational implementation scope outside the vendor contracted responsibility and control, The vendor shall provide process and procedural recommendations for GPA and/or other 3rd party contractors to apply for secure system deployment.
1.6	Third Party Security Review	The vendor shall remediate security issues or vulnerabilities of their System solutions identified by reviews or tests performed by GPA, or a Third-Party Security entity commissioned by GPA, prior to production implementation at the discretion of the and at the vendor's expense.
1.7	Access Control (AC)	
1.7.1	Access Control (AC)	The vendor System solutions shall provide access controls within the system, including but not limited to Access Control Lists, Role Based Access Control (RBAC) models, support of

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

		Active Directory Services (ADS), restricted use notification splash screens, unsuccessful login attempt controls (ref. NIST SP 800-S53 AC-S3, AC-S7, AC-S8).
1.8	Auditable Events	
1.8.1	Auditable Events	The vendor System solutions shall at a minimum, provide logging functionality for the following minimum list of events within the system to support auditing capability by GPA: 1.8.1.1. unsuccessful access attempts 1.8.1.2. configuration file alterations 1.8.1.3. data entry/changes 1.8.1.4. authenticator content alteration 1.8.1.5. maintenance/diagnostics
1.8.2	Content of Audit Records	The vendor System solution logs shall at a minimum contain the following minimum data content items within (ref. NIST SP 800-S53 AU-S3): 1.8.2.1. type of event 1.8.2.2. date and time stamp 1.8.2.3. location of event 1.8.2.4. event success/failure status 1.8.2.5. user associated with event
1.8.3	Response to Audit Processing Failures	The vendor system solutions shall at a minimum log process failures such as but not limited to; event messages no longer being generated/logged, storage space limitations, files being overwritten, etc. (ref. NIST SP 800-S53 AU-S5).
1.8.4	Auditable Event Selection	The vendor system solutions shall at a minimum support functionality for 3rd party tools to select and extract/aggregate event logs by privileged user to support auditable event logging requirements. (ref. NIST SP 800-S53 AU-S12).
1.8.5	System Time Stamps	The vendor system solution shall provide functionality for generating date and time stamps for event logs/audit records based on a system time clock synchronized to a universal/centralized time server based on UTC/GMT to support inter-System audit record reviews and analysis. (ref. NIST SP 800-S53 AU-S8).
1.8.6	Audit Information Protection	The vendor System solution shall provide functionality for protecting audit information/logs and audit tools from unauthorized access, modification, and deletion. (ref. NIST SP 800-S53 AU-S9).
1.8.7	Non-Repudiation	The vendor system solution shall provide functionality for non-Repudiation within the system, such as but not limited to encryption, key management, PKI, hashing, digital signatures, and/or digital message receipts (ref. NIST SP 800-S53 AU-S10).
1.9	Configuration Management (CM)	
1.9.1	Configuration Baselines	The vendor shall apply and provide process controls for establishing, specifying, configuring, documenting, and

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

		verifying accurate System and key components as delivered and updated/upgraded configurations relative to hardware, firmware, software, and settings to support Baseline Configuration Management. When applicable, the vendor systems and components shall be delivered pre-configured in compliance with required configuration baselines. (ref. NIST SP 800-S53 CM-S2).
1.9.2	Configuration Settings Recommendation	The vendor shall provide recommendations for system configuration settings/parameters applicable to the system environments that determine the security state of the System such as but not limited to registry settings, permission settings for accounts/files/directories, and allowed ports/services/protocols/remote connections (ref. NIST SP 800-S53 CM-S6).
1.9.3	Configuration of Least Functionality	The vendor shall provide recommendations for system configuration settings/parameters applicable to the system environments that determine the security state of the System such as but not limited to registry settings, permission settings for accounts/files/directories, and allowed ports/services/protocols/remote connections (ref. NIST SP 800-S53 CM-S6).
1.10	Contingency Planning (CP)	
1.10.1	Contingency Plan Recommendations	The vendor shall provide recommendations for system operational considerations in support of contingency planning and business continuity procedures for effective System recovery after a significant disruption (ref. NIST SP 800-S53 CP-S2).
1.10.2	Contingency Plan Testing Recommendations	The vendor shall provide recommendations for system contingency testing such as but not limited to applicable fault insertions/simulations, test cases, System susceptibilities, troubleshooting checklists, etc. (ref. NIST SP 800-S53 CP-S4).
1.10.3	System Backup Recommendations	The vendor shall provide recommendations for effective System backup and restoration operations (ref. NIST SP 800-S53 CP-S9, CP-S10).
1.11	Identification and Authentication (IA)	
1.11.1	Unique User Identification and Authentication	The vendor system solutions shall provide functionality to support unique identification and authentication of users or processes acting on behalf of users or Systems whether access is via local interfaces or network connections, such as but not limited to, user IDs, passwords, tokens, biometrics, in the case of multifactor methods some combination thereof for uniquely identifying and authenticating users or processes acting on behalf of users whether access is via local interfaces or network connections. Scope of requirement shall include system (workstations, servers, etc.) within System security boundary and applicable external systems/devices (Gateways, Gatekeepers, field tools, mobile

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

		devices, etc.). (ref. NIST SP 800-S53 IA-S2).
1.11.2	Unique Device Identification and Authentication	The vendor system solutions shall provide mechanisms for uniquely identifying and authenticating applicable devices before establishing a connection via network communications (ref. NIST SP 800-S53 IA-S3).
1.11.3	Authentication Content Protection	The vendor system solutions shall provide mechanisms for protecting authenticator content (e.g., passwords) in hashed or encrypted formats from unauthorized disclosure and modification for users, Systems and devices (ref. NIST SP 800-S53 IA-S5).
1.11.4	Authenticator Management	The vendor system solutions shall provide functionality for changing System default authenticators (e.g., back door accesses), authenticator issuance/revocation, and authenticator minimum criteria (e.g., strength, complexity, lifetime, etc.) (ref. NIST SP 800-S53 IA-S5).
1.11.5	Authenticator Obscuration	The vendor system solutions shall provide mechanisms for obscuring authentication content (e.g., passwords) when entering authentication content in authentication windows/dialog boxes (e.g., via masking characters such as asterisks or dots) (ref. NIST SP 800-S53 IA-S6).
1.11.6	Encryption of Authentication Content in Transit	The vendor system solutions shall provide mechanisms for encrypting such as AES-S128, AES-S256, SSL, TLS as minimum standards as applicable for authentication and authorization content during transit between Systems, devices, and to/from authentication servers during authentication processes (i.e., system shall not send passwords in the clear). Any changes to system solution encryption standards shall require approval.
1.11.7	Cryptographic Module Mechanisms	The vendor system solutions shall use mechanisms and cryptographic modules for authentication and authorization that comply with FIPS 140-S2 and comply with encryption requirement 1.9.6 above (ref. NIST SP 800-S53 IA-S7).
1.11.8	Unique User Identification and Authentication (Non-Utility Users)	The vendor shall enforce that their personnel use unique identity user accounts and authentication content for the System accesses whether via local interfaces or network connections (ref. NIST SP 800-S53 IA-S8
1.12	Incident Response	
1.12.1	Incident Response Assistance (IR)	The vendor shall provide technical support should GPA request its assistance in incident response investigations such as forensic activities or incident source determinations related to its system solutions and services (ref. NIST SP 800-S53 IR-S7).
1.13	Media Protection (MP)	
1.13.1	Limit Media Access	The vendor shall attest to protect and limit access to digital and non-digital media to personnel directly involved with the respective systems in accordance with the NDAs and Media Protection Policies and Procedures (ref. NIST SP 800-S53 MP-S2).

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

1.13.2	Media Storage	The vendor shall attest to store system-related digital and non-digital media under controlled conditions in accordance with GPA Media Protection Policies and Procedures (ref. NIST SP 800-S53 MP-S4).
1.13.3	Sanitize Media	The vendor shall attest to sanitize digital and non-digital media, prior to disposal, release out of company control, or release for reuse in accordance with GPA Media Protection Policies and Procedures (ref. NIST SP 800-S53 MP-S6).
1.13.4	Media Disposal	The vendor shall attest to dispose of or return to sensitive or classified information upon the request of GPA and/or at the end of the project in accordance with the Media Protection Policies and Procedures.
1.14	Physical and Environmental Protection (PE)	
1.14.1	Physical and Environmental Protection (PE)	The vendor shall comply with GPA Physical Access Control Policies and Procedures (ref. NIST SP 800-S53 PE-S3).
1.15	Personnel Security (PS)	
1.15.1	Personnel Screening	The vendor shall provide proof of background checks which require ID and 7-Syear criminal background checks for their personnel and any 3rd party contractors they provide for working within GPA facilities/premises, using GPA property, and/or using remote network connections to access systems in accordance with establish policies (ref. NIST SP 800-S53 PS-S3).
1.15.2	Access Agreements	The vendor shall enforce that their personnel and any 3rd Party personnel they contract, sign access agreements prior to being granted access to utility facilities (ref. NIST SP 800-S53 PS-S6, PS-S7).
1.16	Systems and Services Acquisition Policies and Procedures (SA)	
1.16.1	Administrator Documentation	The vendor shall provide administrator level documentation for their system solutions that describe secure configuration, installation, and operation of the system (ref. NIST SP 800-S53 SA-S5).
1.16.2	User Documentation	The vendor shall provide user-level documentation for their system solutions that describe user accessible security features/functions, and how to effectively use and maintain those system features/functions (ref. NIST SP 800-S53 SA-S5).
1.16.3	Known vulnerabilities	The vendor shall provide information on known vulnerabilities of their system solutions regarding configuration and use of administrative (i.e., privileged) functions (ref. NIST SP 800-S53 SA-S5).
1.16.4	Security Development Lifecycle Methodologies	The vendor shall apply and be able to provide artifacts of security methodologies that satisfy the intent and implement the core concepts of a formal Security Development Lifecycle (SDL) in their requirements, development, test, integration,

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

		implementation, documentation, and ongoing support of their system solutions and services. SDL is a security assurance process framework based on education/training, continuous process improvement, and accountability that embeds/integrates security and privacy (data sensitivity) criteria in all phases of the development lifecycle (requirements, design, implementation, verification, release, response) and includes security engineering specific criteria in the application/execution of requirements, design, quality gates, risk assessments, threat modeling, tools, testing, attack surface analysis/minimization, reviews, documentation, and incident response plans (ref. NIST SP 800-S53 SA-S8).
1.16.5	External System Information Services	When the vendor requires remote network connectivity (e.g., VPN) to Electra SCADA systems, the vendor shall comply with GPA security standards and policies that include but are not limited to configuration management, testing, access management, and boundary protection (ref. NIST SP 800-S53 SA-S9).
1.16.6	Developer/Integrator Configuration Management	When the vendor provides system developer and/or integrator services to GPA, the vendor shall perform and document the following (ref. NIST SP 800-S53 SA-S10):
1.16.6.1	Configuration Management	Perform configuration management during system design, development, implementation, and operation services.
1.16.6.2.	Change Control	Manage and control changes to the system.
1.16.6.3.	Approved Changes	Implement only approved changes to the system.
1.16.6.4.	Approved Change Documentation	Document approved changes to the system.
1.16.6.5.	Security Flaw Tracking	Track security flaws and flaw resolution.
1.16.7	Developer/Integrator Testing	Test plan which includes a backout plan.
1.16.7.1	Security Test Criteria	The vendor shall provide security specific test criteria, test cases, evaluation, and test support for all required test phases of the implementation of their System solutions
1.16.7.2.	Flaw Remediation Process	Implement a verifiable flaw remediation process to correct security weaknesses/deficiencies identified during security testing and evaluation processes.
1.16.7.3.	Test Results Documentation	Document results of the security testing/evaluation and flaw remediation processes.
1.17	System and Communications Protection (SC)	
1.17.1	Boundary Protection	The vendor system solutions shall include mechanisms to monitor, detect, alert, control, and protect against attempts to compromise communications integrity at key internal boundaries within the system (ref. NIST SP 800-S53 SC-S7).
1.17.1.2.	Boundary Protection External Recommendations	The vendor shall secure implementations of their external boundaries (ref. NIST SP 800-S53 SC-S7, CA3).
1.17.2	Cryptographic Usage	The vendor system solutions shall use cryptographic

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

		mechanisms and modules that comply with FIPS 140-S2 and apply encryption standards such as AES-S128, AES-S256, SSL, TLS as minimum standard applicable for maintaining data integrity within the system. Any changes to system solution encryption standards shall require approval by GPA (ref. NIST SP 800-S53 SC-S13).
1.18	System and Information Integrity (SI)	
1.18.1.	Flaw Remediation	The vendor shall provide and apply processes, mechanisms, and procedures for the identification, documentation, and remediation of system flaws (ref. NIST SP 800-S53 SI-S2)
1.18.2.	Remediation Testing	The vendor shall document, and test software updates related to flaw remediation (i.e. patches, service packs, hot fixes) for effectiveness and potential adverse side effects prior to installation on GPA systems (ref. NIST SP 800-S53 SI-S2).
1.18.3	Configuration Considerations	The vendor shall incorporate system changes due to flaw remediation into the System configuration management process (ref. NIST SP 800-S53 SI-S2).
1.18.4	Malicious Code Protection Recommendations	The vendor shall provide technical guidance and recommendations to GPA on the applicability and usage of malicious code protection applications (e.g., anti-malware, anti-virus) and other system hardening measures on the vendors systems so as not to introduce negative impacts or degradations to system functionality, performance, and/or risks to system availability due to response to false positives as a result of adding subject protective measures (ref. NIST SP 800-S53 SI-S3).
1.18.5	System Security Alerts, Advisories, and Directives	The vendor shall notify GPA of any security alerts, advisories, and/or directives applicable to their system solutions in a timely and responsive manner (ref. NIST SP 800-S53 SI-S5).
Trade Agreements Act (19 U.S.C. & 2501-2581).		
1	TAA	The vendor shall confirm that acquire products that are produced or undergo a "substantial transformation" within the United States or from a designated TAA country.
2	TAA	The vendor shall confirm specifically the major components, are designed, manufactured, assembled, tested, and supported in the United States from US and international components.
3	TAA	The vendor shall confirm that acquired goods and/or services is wholly the growth, product, or manufactured of the United States or a designated country.
4	TAA	The vendor shall confirm that acquired goods has not been substantially transformed in the United States or a designated country into a new or different article of commerce with a name, character, or use distinct from that of the article from which it was transformed
5	TAA	The vendor shall confirm that acquired service firm that is

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

		providing services is established in the United States or a designated country.

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

7 Approvals

By signing below, I certify that I have read, acknowledged and approved all sections of this document.

Approved by: _____ Date: _____

This document is for official use only. This document must be handled in a confidential manner at all times. Distribution and/or reproduction of this document outside the intended and approved use is strictly prohibited.

INVITATION FOR BID

ISSUING OFFICE:
Guam Power Authority-Procurement Office
1st. Floor, Room 101
Gloria B. Nelson Public Service Building
688 Route 15
Mangilao, Guam 96913

Attn: JOHN M. BENAVENTE, P.E.
General Manager
c/o JAMIE LYNN C. PANGELINAN
Supply Management Administrator

5/12/2023
for **JOHN M. BENAVENTE, P.E. DATE**
General Manager

DATE ISSUED: **12/01/2022** **12/08/2022** MULTI-STEP
BID INVITATION NO.: GPA-012-23

BID FOR: Renewable Energy Resource Acquisition Phase IV

SPECIFICATION: SEE ATTACHED

DESTINATION: SEE ATTACHED

REQUIRED DELIVERY DATE: SEE ATTACHED

CUT-OFF DATE FOR RECEIPT OF QUESTIONS: 4:00 P.M., Tuesday, February 7, 2023

INSTRUCTIONS TO BIDDERS:
INDICATE WHETHER: _____ INDIVIDUAL _____ PARTNERSHIP _____ CORPORATION

INCORPORATED IN: _____

✱ This bid shall be submitted in the form of, **one (1) original, six (6) bound copies of their bid including one completed electronic copy on one disk of the Qualitative Scoring Workbook including all addenda,** if any to the issuing office above no later than **(Time) 2:00 P.M. (Guam CHamoru Standard Time; ChST), Date: August 18, 2023**. **Once completed electronic copy on another disk of the Price Proposal Workbook by the "Cut-off Date for Receipt of Priced Proposals". Bidders are advised to keep a copy of the completed Workbooks and test the electronic copies on disks prior to submitting them to GPA.** Bid submitted after the time and date specified above shall be rejected. See attached General Terms and Conditions and Sealed Bid Solicitation for details.

The undersigned offers and agrees to furnish within the time specified, the articles and services at the price stated opposite the respective items listed on the schedule provided, unless otherwise specified by the bidder. In consideration to the expense of the Government in opening, tabulating, and evaluating this and other bids, and other considerations, the undersigned agrees that this bid remain firm and irrevocable **not less than eight (8) months after the Bid Submittal Closing Date.**

NAME AND ADDRESS OF BIDDER:

SIGNATURE AND TITLE OF PERSON AUTHORIZED TO SIGN THIS BID:

AWARD: CONTRACT NO.: _____ AMOUNT: _____ DATE: _____

ITEM NO(S). AWARDED: _____

CONTRACTING OFFICER:

JOHN M. BENAVENTE, P.E. DATE
General Manager

NAME AND ADDRESS OF CONTRACTOR:

SIGNATURE AND TITLE OF PERSON

1. OVERVIEW

In this Invitation for Multi-Step Bid ("IFB"), GPA is seeking competitive bids for renewable energy resources to meet a portion of its overall resource needs. For selected Bidder(s), GPA will execute purchase power agreements for delivery of firm, non-intermittent power from one, or more, renewable generation resources to the 34.5 kV or 115 kV GPA transmission system. GPA intends to procure a total minimum annual energy of 300,000 MWh up to 530,000 MWh (approximately 180 MW to 320 MW), based on proposed sites, in this Phase IV acquisition that can meet the following established requirements:

- **RENEWABLE RESOURCE TECHNOLOGY:** The Bidder's resource technology shall be grid-forming / black-start capable and meet the definition of "renewable resource" as described in ***Section 2.2.1 Acceptable Renewable Technologies***.

* - **ENERGY AND CAPACITY:** The renewable energy resource shall deliver an annual minimum energy (AC) as specified in the Bidder's Qualitative Proposal with a maximum export capacity of 60 MW (AC) at the interconnection point; this may be a combination of several generation units at one or more sites. However, the nameplate capacity that can be installed may be higher than 60 MW, subject to the maximum additional MW capacity that the GPA system can handle as determined by a System Integration Study. The System Integration Study will be completed within 120 days after evaluation of the Price Proposal(s) and initial notification of the most qualified Bidders. For proposals with an intermittent renewable energy resource coupled with an energy storage system, GPA will allow 60% of the resource to be DC-coupled to the energy storage system with the remaining 40% AC-coupled to the GPA grid. Therefore, 60% of the total project capacity will deliver firm, energy-shifted power from the energy storage system to the GPA grid. The energy storage system shall also provide ramp-rate control for the power delivered from 40% of the total project capacity such that the ramp-rates are kept within 1% per minute at the guaranteed success rate of 95% during the energy production period. However, before or after a GPA curtailment, this rate may be exceeded at the request of the GPA Power System Control Center operators. GPA will not pay for the energy delivered to the GPA grid that did not meet the guaranteed success rate.

- **DISPATCHABLE ACTIVE POWER CAPABILITY:** The active, or real, power of the renewable energy resource shall be dispatchable at the point of interconnection, between the hours of 6:00 PM to 6:00 AM, as required by the GPA Power System Control Center operators or a SCADA control point. The available capacity may also be dispatched outside of these hours if deemed necessary by the GPA Power System Control Center operators. The delivered output to the GPA grid shall be firm, non-intermittent power with a ramp-up and ramp-down rate limited to 1% of rated power output per minute. However, this rate may be exceeded at the request of the GPA Power System Control Center operators. The total capacity and energy available for dispatching shall be provided to the GPA Power System Control Center through a SCADA point every second.

- **DISPATCHABLE REACTIVE POWER CAPABILITY:** The renewable energy resource must provide a dispatchable reactive capability requirement up to 0.80 lag to lead at the point of interconnection as required by the GPA Power System Control Center operators and a SCADA / grid controller automated

output point. The project shall perform at +/- 0.80 PF Dynamic Range up to and including the maximum MW output and shall not reduce reactive capability near the peak real power output.

- **INTERCONNECTION:** The renewable energy resource shall deliver energy directly to the existing GPA 34.5 kV or 115 kV transmission systems, subject to the result of a System Integration Study to be completed after Step 2 of the proposal evaluation. Interconnection to the 115 kV transmission system near the Apra Substation or Harmon Substation is preferred.

* - **ENERGY STORAGE SYSTEM (ESS): T**he renewable energy resource shall be equipped with an energy storage system (ESS) that meets GPA's requirements as described in **Section 2.2.2 Acceptable ESS Technologies.** The ESS must provide the following primary functions:
  - **ENERGY-SHIFTING:** The primary purpose of the ESS shall be for energy-shifting, which is to deliver the energy produced at another time or period of the day.
  - **RAPID RESERVE:** The additional function of the ESS is to provide rapid reserve in response to under-frequency events. The total energy exported for these events shall be included in the annual minimum energy requirement.
  - **RAMP-RATE CONTROL:** In this mode, the ESS will supply or absorb real power at the point of interconnection in an attempt to control the power output of the renewable energy resource which is AC-coupled to the GPA grid such that the ramp-rate is limited based on the ramp-rate setpoint. Sufficient SOC management control must be provided for optimal ramp-rate control. Manual and remote changes to the ESS ramp-rate setpoint shall also be allowed if needed.

Bidders shall also provide the other grid services in the table below:

Grid Service	Description
Firm Power Dispatch	Provide Dispatchable Renewable Energy
Operating Reserve	Standby Generation Reserve
Fast Frequency Regulation	Rapid injection or absorption of power in response to changes in frequency to maintain system frequency within a tight bandwidth
Rapid Reserve	Respond to fast frequency decay due to trip of large generators on the GPA system by immediate injection of power to the grid to balance generation and demand and prevent underfrequncy load shedding.
Shaping and Firming	Smoothing out intermitency of the renewable resource.
Black Start	Capability to Black Start other Generators over the Transmission System
Grid Forming	Capability to form and supply Microgrids post-natural disaster (i.e., typhoons) or system blackouts.
Energy Shifting	Long Duration Energy Storage System Function
Volt/Var Optimization	Steady state and dynamic management and optimization of Power System Voltages

- **COMMERCIAL OPERATION HISTORY:** The technology proposed for the renewable resource shall have at least one (1)-year of commercial operations history in a utility environment.
- **COMMERCIAL OPERATION COMMENCEMENT:** The renewable energy resource shall be available for commercial operation within thirty-six (36) months from the contract execution.
- **CONTRACT TERM:** The renewable energy resource shall provide energy for a term of 20 years, with the option to extend for two additional five-year terms, for a maximum term of thirty years.
- **BUY-OUT OPTION:** GPA intends to reserve the option to buy-out the capital portion of the contract. Bidders must provide a buy-out schedule for each contract year.
  - GPA reserves the option to take a percent equity in stakes in the project at any time; such percent equity in stakes will be applied against the buy-out amount.
  - GPA and the successful bidder(s) shall negotiate the buy-out percent if the option is taken.
  - The bidder must provide a year-by-year schedule of reduction in energy fees as a function of the contract year buy-out and 25%, 50%, 75%, and 100% of equity stake taken by GPA.

2. DESCRIPTION