Republic of the Philippines
Office of the Solicitor General
134 Amorsolo St. Legaspi Village, Makati City

Technical Working Group for
Information and Communications Technology

TERMS OF REFERENCE

Supply and Delivery of Security Key (For strong multi-factor and password-less authentication)

Background:

The Office of the Solicitor General (OSG) is the principal law office and legal defender of the Government and the People's Tribune, securing justice for the nation through excellence in legal advocacy. Given the sensitive nature of the information handled and the need for robust cybersecurity measures, the OSG recognizes the importance of enhancing its security posture. One essential component of this effort is procuring physical security keys (for strong multi-factor and password-less authentication), which will provide an additional layer of protection for accessing systems and sensitive data.

Objective:

The objective of procuring physical security keys for the Office of the Solicitor General is to strengthen cybersecurity by implementing two-factor authentication (2FA) for authorized personnel. This procurement aims to:

1. Enhance Security: Security keys will bolster access control and authentication processes, reducing the risk of unauthorized access and potential data breaches.
2. Safeguard Sensitive Information: Using security keys, OSG seeks to protect confidential legal documents, sensitive case information, and other critical data from unauthorized access or cyber threats.
3. Ensure Compliance: The procurement aligns with industry best practices and regulatory requirements related to information security, ensuring OSG's adherence to data protection standards.
4. Mitigate Insider Threats: Security keys will help mitigate insider threats by requiring physical presence for authentication, reducing the risk of compromised credentials.
5. Improve Operational Efficiency: Security keys offer a convenient and efficient method for multi-factor authentication, streamlining access for authorized personnel while maintaining a high level of security.

The procurement of security keys for the Office of the Solicitor General is a proactive measure to fortify cybersecurity defenses and safeguard the integrity of legal proceedings and sensitive government information.

Terms:

1. *Scope.* - Supply and delivery of Security Keys

2. *Approved Budget for the Contract (ABC).* – The ABC is **Three Million and Four Hundred Thousand Pesos (₱3,400,000.00)** inclusive of all government taxes, charges, and other standard fees.

MOOE-SEMI EXPANDABLE			
ITEM	**QTY**	**UNIT COST**	**TOTAL**
Security Key (for strong multi-factor and password-less authentication)	**850**	4,000.00	3,400,000.00
		TOTAL	**₱ 3,400,000.00**

3. *Delivery.* - All items should be delivered within 30 days of receipt of the Notice to Proceed.

4. *Training.* -

   a. The Supplier must provide the necessary comprehensive training/knowledge transfer program for the end users within ten days of solution delivery.

   b. The training must be conducted during business hours and coordinated with Case Management Service (CMS). The CMS will provide certification for delivery and training completion.

   c. The course outline, training materials, product guides, and documentation should be available online, with soft copy delivered to CMS.

5. *Schedule of Payment.* – To guarantee the performance by the winning bidder of its obligations under the contract, it shall post a performance security before the signing of the contract. The performance security shall be in an amount not less than the required percentage of the total contract price in any of the following forms and accordance with the following schedule:

Form of Performance Security	Amount of Performance Security (Not less than the required % of the Total Contract Price)	Statement of Compliance
a) Cash or cashier's/ manager's check issued by a Universal or Commercial Bank.	5%	

b) Bank draft/ guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank; *however,* it shall be confirmed or authenticated by a Universal or Commercial Bank if issued by a foreign bank.	**5%**	
c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	**30%**	
TERMS OF PAYMENT		**Statement of Compliance**
Supplier agrees to be paid based on a progressive billing scheme as follows:		
• Within thirty days from completion of the delivery and issuance of the Inspection and Acceptance Report by the OSG and submission of all other required documents – 95% of the contract price. • One year from the issuance of the Inspection and Acceptance Report by the OSG – 5% of the contract price.		

All bid prices shall be considered as fixed prices, and, therefore, not subject to price escalation during contract implementation.

6. *Qualifications of the Supplier.* -

a. The Bidder shall have a Single Largest Completed Contract (SLCC) that is at least one (1) contract similar to the Project the value of which, adjusted to current prices using the PSA's Consumer Price Index, must be equivalent to at least fifty percent (50%) of the ABC, completed within 5 years prior to the deadline for the submission and receipt of bids.

For this purpose, similar contract shall refer to the procurement contract of any ICT security device.

b. The bidder shall submit a valid and current Certificate of Distributorship/Dealership/Resellership of the product being offered, issued by the principal or manufacturer of the product (if the bidder is not the manufacturer). If not issued by the manufacturer, they must also submit a certification/document linking the bidder to the manufacturer.

c. The bidder must attach a brochure of the brand being offered.

d. The bidder must have a main office or satellite office in or around Metro Manila and/or nearby provinces.

e. The bidder shall submit documents relevant to the project, such as but not limited to the following:

- Valid DTI or SEC Registration;
- Valid and Current Mayor's Permit/Municipal License;
- Valid and Current Business Permit;
- Tax Clearance Certificate as finally reviewed and approved by BIR;
- Statement of contracts completed which are similar in nature to the contract to be bid.
- Net Financial Contracting Capacity (NFCC) Computation

7. *Warranty/ Product Support Requirement. -*

The Service provider should provide a notarized undertaking that it will provide the warranty/after-sale support requirement, as follows:

a) Provide one (1) year of standard support services.
b) For technical assistance, the contact person would be designated by the provider and support through email/online/phone for the entire standard support services.
c) The winning bidder must provide eight (8) hours x five (5) days of technical support through unlimited phone, email, remote, and chat.
d) The highest bidder must have a high priority level for the support available eight (8) hours x five (5) days with unlimited phone, email, remote, and chat assistance.
e) The winning bidder will provide technical support covering the following but not limited to:
    - Online incident submission;
    - Less than 4 hours response time upon receipt of the request from OSG;
    - Consulting services on related support and services.

Compliance with the Government Procurement Reform Act

8. *Applicable Law. -*

1. Applicable provisions of the Government Procurement Reform Act (RA No. 9184) and its Revised Implementing Rules and Regulations (RIRR) shall be deemed integrated to the Terms of Reference (TOR).

9. *Construction.* – In case of conflict between a general term and a specific provision, technical or otherwise, the latter shall prevail.

Technical Specifications:

PARAMETERS	SPECIFICATIONS	COMPLIANCE
Supplier Keys General Compliance	Hardware Token-Based Security	
	Support Passwordless Operations for secure, simple login.	
	Capable of supporting Single-factor, two-factor, or multi-factor authentication	
	Support NFC tap authentication.	
Supplier Keys must be compliant with the following authentication protocols.	FIDO U2F	
	FIDO2	
	PIV/Smartcard	
	OATH HOTP	
	OATH TOTP	
	Security Key OTP	
	Challenge Response	
	Open PGP	
Supplier Keys must be compatible with the following multiple mediums	USB A	
	NFC	
Works on all major operating systems	Microsoft	
	Linux	
	MAC	
	iOS	
	Android	
Supplier Keys must be highly durable and convenient for users	Dustproof and water resistant	

Supplier Keys must be highly durable and convenient for users	Crushproof	
	No moving parts	
	No signal dependency or battery for mobile-free and restricted environments	
	Suppliers' keys should have the option of a key chain.	
	USB Port Durability	
Warranty	1 year on parts and labor.	

(nothing follows)