ANNEX A: TERMS OF REFERENCE

SERVICE FOR THE CYBERSECURITY MANAGEMENT
(DATA PRIVACY READINESS ASSESSMENT, COMPLIANCE, AND SECURITY GOVERNANCE)

I. BACKGROUND

Technology has played a significant role in the evolution of good governance. It is proven that the effects of technology on governance increase transparency, information sharing, and accountability. This prompted organizations or agencies in the government to race against digital transformations in having their systems online, ease of access to information, and real-time management collaborations. Along with the effects of this so-called Digital Transformation is the possibility of data loss, system breach, and cyber-related incidents that may violate anyone's right to data privacy.

The enactment of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring the free flow of information to promote innovation and growth. It also recognizes the State's inherent obligation to provide personal information in information and communications systems in the government and the private sector, which is secured and protected. The National Privacy Commission (NPC) provides guidelines for processing personal information and appropriate levels of security protection, which the agencies and organizations must comply with.

On the other hand, the Department of Information and Communications Technology (DICT) published the government National Cybersecurity Plan (NCSP) 2022, which provides the security of information guidelines, policies, and programs that each government agency must take part in policing and safeguarding the cyberspace against cyber threats.

The project requires Solution Providers to aid in the objective compliance of the Data Privacy Act requirements by assessing the TPB's ICT plans and programs, policies, processes, systems, technology, people, and other management information systems that will be found vulnerable and may contribute risk in the implementation of data privacy protection and security. It involves the provision of documentation, policing, risk assessment, and recommendations that will improve the level of TPB's ICT service delivery, security, and protection.

II. OBJECTIVES

The project aims for the TPB's compliance with the requirements of the Data Privacy Act by strengthening the TPB's ICT frameworks, policies, and processes by meeting the following objectives:

- Establish the policy, guidelines, and standards to govern the ICT Framework and DPA Privacy Governance;
- Assess the information technology systems and network infrastructures and make necessary recommendations on TPB information security posture through formulating Policies on Information Security Management System (ISSM) and Cybersecurity Management System (CMS)

to protect Data Information as required by the Data Privacy Act.

- To test and verify the security of the information technology systems and network infrastructure to ensure the effectiveness of deployed security measures as they compare to security best practices, business objectives, and regulatory requirements

- Analyze findings, prepare documentation to provide a detailed analysis of the desired security posture with industry best practices, and provide a prioritized action plan.

- Identify and recommend safeguards suited to the Agency's environment to strengthen privacy, confidentiality, security policies, guidelines, standards, processes, and procedures, and incorporate new approaches as needed or required.

III. SCOPE OF WORKS / SERVICES

Item / Type	Scope of Works / Services	Description
1 SERVICE	Must conduct an initial meeting or kick-off with stakeholders to discuss the schedule, timeline, criteria, personnel , and other requirements embodied in the Project Management Implementation Plan	A Project Management Implementation Plan is a document discussed during project initiation or kick-off. It provides a comprehensive baseline of what is to be achieved by the project, how it is to be achieved, who is involved, how it will be reported and measured, and how the information will be communicated. It will be used as a reference for any decision made on the project and for clarifications of unclear areas. This is to ensure that the management of the project is carried out consistently and in line with policies and procedures. It usually includes an executive summary, strategic or organization alignment, project scope definition, feasibility assessment and contingency plans, constraints, human resource requirements, material or equipment requirements, project schedule and milestones, budget or cost estimates, risk management, project issues, change management, communications management and related products and deliverables (known dependencies), approval and necessary attachments. Although this document is required in the project kick-off or initiation phase, it is also a living document that evolves as the project progresses and should be updated for any relevant information.

2 / TRAINING	Facilitate the attendance for capacity building of TPB personnel for the sustainability of the TPB Privacy Management Program	Facilitate the conduct or the attendance of identified TPB personnel to the following training (face to face or online) programs: a. Data Protection Officer or GPDR Data Protection Officer Training or its equivalent; b. DPO Audit or ISO 27701 Lead Auditors c. Training or its equivalent; and d. VAPT Training or its Equivalent.
3 / TRAINING	Facilitate the conduct of Data Privacy Awareness through orientation, training, seminars, workshop, and creation of Audio-Video Presentation Campaign	Must be able to provide an Awareness Seminar Program for the Heads of each department which concerns Personal Information Must be able to provide Certificate of Attendance for the attendees of the seminar program. Produce and/or deliver at least 5 mins AVP presentation on TPB DPA Awareness Campaign tailored to TPB settings.
4 / SERVICE	Conduct Vulnerability Assessment and Penetration Testing of the TPB Systems Infra and Infostructure	Facilitate or conduct penetration and vulnerability assessment for engagement involving network infrastructure and web applications service by synthesizing information collected during interviews, documentation review, workshops to prepare roadmap to close the highest critical and medium risk in focus areas with an objective and measures of success that defines the assessment suitable to TPB requirements or processes, such as: a. Identification of critical vulnerabilities – physical, cyber and interdependencies and development of appropriate response b. Identify and rank all key assets form a security perspective c. Develop the business case for making security investments and organizational changes that will enhance security d. Enhance awareness and make security as integral part of privacy management programs Following are the recommended assessment criteria, methodology and focus areas for the conduct of Vulnerability Assessment and Pentest; 1. **Pre-Assessment Phase**, VAPT Assessment criteria – defines objectives and scope of assessment, establish information procedures and

identify and rank critical assets this is done thru identification of requirements thru information gathering and interview.

2. **Assessment Phase**,
   Conduct of Vulnerability Assessment and Penetration Testing in the following:
   a. Assessment of Network and Infrastructure
   b. Assessment of Websites
   c. Assessment for Physical Infrastructure Security

Assessment Process shall cover the following:

VA	**PENTEST**

VA involves information gathering, network scanning and vulnerability identification, such as,
• Reconnaissance or Information Gathering (Enumeration of information from Network and web applications)
• Network Mapping this involves scanning of port, vulnerability and network map
  ○ Port scanning targets the information like open ports, live streams an various service running on the host;
  ○ Vulnerability
	This includes manual or automated tool based pentesting which includes the following:
	• Gaining access and privilege phase where penetration breaks into the system / network using various tools or methods. After entering into the system, attacker has to increase his privilege to administrator level so he can install an application he needed or modify nor hide data
	• Maintaining access this phase, attacker or penetrator may hack the system to show it was vulnerable or he can be so mischievous

		Scanning – checks the target weaknesses which can be exploited; ○ Network mapping – is finding the topology of network, routers, firewalls servers and host information and drawing the network diagram with available information. This diagram may serve as a valuable piece of information thought the penetration process. • Vulnerability Identification such as misconfiguration and vulnerabilities detection, patches, default password or password guessing, unwanted ports and weakness of devices and servers	that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using trojans, • rootkits, or other malicious files. The aim is to maintain the access or escalate further its privileges and gather more information to the target until he finishes his planned task to accomplish. Clearing Tracks – this phase is for a penetrator not to get caught. Intruder always clears all evidence so that in later point of time no one will find any traces leading into him. This involves modifying, corrupting or deleting values or logs, auditing, registry and installing applications used or deleting all folders created	
		3. **Post Assessment Phase**, i Is where findings, priorities and recommendations is presented thru report (See Annex D).		
5 / SERVICE	Assessment Report on TPBs Information System Strategic Plan	Conduct of 3rd party review, assessment and report on TPB ISSP relative to DPA compliance, protection and related programs, *eGov Masterplan and related governance standards.*		
6 / SERVICE	Adapt DICT's Policies on Information Security Management System (PIMS) and Cybersecurity Management System (CMS)	Draft policies for TPBs Information Security Management System and Cybersecurity Management System. Content must be in accordance with ISO 27001 guidance and TPB policy format.		

7 / SERVICE	Assessment of the organization's current status with regards to DPA compliance and provide a documentation for Project Charter. Must provide DPA Gap Analysis Documentation after initial assessment of the organization's current status	Facilitate DPA readiness and compliance thru the conduct of Consultation, Interview, Focus Group Discussion, Meetings, and Workshop to gathering relevant information, process validation, gaps analysis and assessment to come up with appropriate recommendations and report documentation.
8 / SERVICE	Conduct DPA Privacy Impact Assessment (PIA), formulation and Approval of PIA Report	PIA is an instrument for assessing the potential impacts on privacy of process, information system, program, software module, device or other initiative which processes personal information and in consultation with stakeholders, for taking actions as necessary to treat privacy risk.
		For this purpose, NPC PIA Toolkit and ISO/IEC 29134:2018 will be used for the conduct of PIA. Reports may include documentation on measures taken for risk treatment and measures arising from the use of information security management system (ISMS) or the ISO/IEC 27001.
		Must be able to accomplish the organization's Personal Data Inventory;
		Must provide assessment and inventory of the organization's Data Processing Systems, may it be manually or automatedly generated or processed.
		Must assist in drafting the required documents for the registration of data processing systems
9 / SERVICE	Draft Data Privacy Manual and Data Privacy Governance Cycle or Privacy Management Program of the TPB	Must assist in drafting the Data Privacy Manual, provide assistance in drafting and/or reviewing the Privacy Notices. Must assist in drafting the Privacy Management Program and Plans as well as the creation of the breach management Team
		Must be able to assist in the appointment of the breach management team members, their roles and responsibilities
		Must take the lead in reviewing existing Privacy Policies and Procedures. As part of this process, Must explore encryption solutions to ensure data privacy compliance.

		Additionally, Must document the potential for implementing blockchain technology to maintain data integrity.
10 / SERVICE	Simulation Exercises on Breach Reporting and Management	Must be able to provide an Breach Reporting and Management Exercises among stakeholders

IV. BIDDERS QUALIFICATION

item	Qualifications	Description	Remarks
1	Experienced, reliable, established Company	• Must have at least five (5) years as an ICT company preferably a System Integrator Company or Similar	PHILGEPS Platinum
2	Government Accreditation	• Recognized as Cybersecurity Assessment Provider for Vulnerability Assessment/Penetration Testing (VAPT) and Information Security Management System (ISMS) by the Department of Information and Communications Technology	Valid and updated VAPT and ISMS certification issued by DICT
3	Data Confidentiality Capability	• Has Created an Encryption Tool for data confidentiality	Certification of developed encryption tool. Must be available and working.
4	Data Availability Capability	• Has Developed Anti-DDOS and Web application firewall Solutions and implemented them in the last three years. • Vendor should have developed their own Web application Firewall and cyber security services • Vendor should have its own Anti-DDOS services and must provide Certification	Certification of developed Anti-DDOS and Web Application Firewall Solutions. Must be available and working.
5	Big Data Implementation Capability	• Implemented Data and Command Centers in both private and public organizations	Certification of Implemented Data and Command Centers in both private and public

			organizations
6	Project and Service Management	• Implemented Support Management System • Project Management Certification	Valid ITIL Certification Valid Project Management Certification
7	Infrastructure Management and Certification	• Engineer's certification (i.e LPIC, RHCE) with relevance to the platform must be issued by an association recognized internationally.	Certification of any infra or Operating System related
8	Database Certification	• Must Provide Database Certification	Valid Database Administrator Certification
9	Cyber Security Certification	• Ethical Hacking Certification • Blockchain Certification	Valid Hacking Certification or Blockchain Certification

V. MANDATORY TECHNICAL REQUIREMENTS

In addition to the required technical requirements, the bidder shall also submit the following documents.

1. Company Profile, which indicates, among others, a summary of services rendered by the firm and years of existence in the industry;
2. Curriculum Vitae of the proposed workforce to be deployed to the project;
3. Proposed Methodology, to include the
   (a) Approach and Method,
   (b) Work Plan,
   (c) Gannt Chart, and
   (d) Organization and Staffing

VI. CONFIDENTIALITY, LIABILITY, AND NON-DISCLOSURE AGREEMENT

1. Data Confidentiality

Any information or document obtained from TPB, including but not limited to any obligations before the termination or expiration and provisions on confidentiality and proprietary rights, will remain in effect after the services rendered to TPB. Hence, the undertaking of the bidder not to disclose and to keep the information confidential shall exist even after the expiration or termination of his services to the TPB, nor can the bidder, at any time, disclose that the TPB engaged his services for its project.

2. Proprietary Rights

Records and other documents, reports, and relevant data, such as diagrams, plans, designs, estimates, specifications, and other supporting records of materials the HoPE compiled and prepared in the course of the performance of the services, shall be exclusively owned by TPB

and shall not be used by the bidder for purposes not related to this agreement, without prior written approval of the HoPE.

VII. PROJECT ACCEPTANCE AND CLOSEOUT

Project Closing Workshop and turnover ceremony shall be conducted upon project completion.

Consultant shall submit a Terminal Report documenting all activities engaged in project implementation. It includes challenges, best practices, recommendations, resolutions, and lessons learned among the stakeholders.

Certificate of Acceptance shall be issued duly signed by the Project Sponsor upon endorsement and recommendation of the Project Manager upon receipt of the Terminal Report and relevant documents attached, particularly those produced throughout the project duration and turn-over of documents.

Project Closing Workshop and turnover ceremony shall be conducted upon project completion.

Consultant shall submit Terminal Report documenting all activities engaged in project implementation. It includes challenges, best practices, recommendations, resolutions, and lessons learned among the stakeholders.

Certificate of Acceptance shall be issued duly signed by the Project Sponsor upon endorsement and recommendation of the Project Manager upon receipt of the Terminal Report and relevant documents attached, particularly those produced throughout the project duration and turn-over of documents.

VIII. TIMELINE

The project will commence after the receipt of the issuance of NTP.

Item	Scope of Works/Services	Description	Timeline (Month 1-3)
1	Initial Kick-Off Meeting	Conduct an initial meeting with stakeholders to discuss the Project Management Implementation Plan.	Month 1, Week 1
2	Capacity Building for TPB Personnel	Facilitate data protection and VAPT training programs for TPB personnel.	Month 1, Weeks 2-3
3	Data Privacy Awareness Program	Conduct awareness programs and create AV presentations for	Month 1-2

		data privacy.	
4	Vulnerability Assessment and Penetration Testing	Perform assessments on TPB systems to identify vulnerabilities and enhance security awareness.	Month 1-2
5	Information System Strategic Plan Review	Review and report on TPB's Information System Strategic Plan for data privacy compliance.	Month 2
6	DPA Compliance Status Assessment	Assess TPB's current data privacy compliance status and produce gap analysis documentation.	Month 2-3
7	DPA Compliance Status Assessment	Assess TPB's current data privacy compliance status and produce gap analysis documentation.	Month 2-3
8	Privacy Impact Assessment	Conduct and approve PIAs using NPC PIA Toolkit and ISO/IEC 29134:2018.	Month 2, Week 4 to Month 3, Week 1
9	Drafting of Data Privacy Documents	Assist in creating the Data Privacy Manual and Privacy Management Program.	Month 3, Weeks 1-2
10	Breach Reporting and Management Simulation	Conduct breach management exercises for stakeholders.	Month 3, Weeks 3-4

IX. PAYMENT SCHEME (must be approved by TPB)

Terms	Description	Deliverables/Milestones	Due by	Percentage of Total Payment
1st Tranche	Project Initiation and Training Programs Kick-Off	Successful initial kick-off meeting Completion of Data Protection Officer Training or its equivalent for TPB personnel	Month 1, Week 3	15 %
2nd Tranche	Privacy Awareness and Security Assessment Completion	Completion of Data Privacy Awareness Program Final report on Vulnerability Assessment and Penetration Testing	Month 2, Week 4	20%
3rd Tranche	Strategic Compliance Documentation	TPB approved final draft of TPB Information Security Policies DPA Gap Analysis Documentation Privacy Impact Assessment Report	Month 3, Week 2	50%
4th Tranche	Finalization and Simulation Exercises	TPB approved final draft of the Data Privacy Manual and Privacy Management Program Completion of Breach Reporting and Management Simulation Exercises	Month 3, Week 4	15%

The supplier is encouraged to have a Landbank account. Payment shall be made through LBP bank deposit. If the supplier does not have a Landbank account, the supplier shall shoulder bank charges.

Send the bill of actual expenses to the **TOURISM PROMOTIONS BOARD** addressed to **COO MARIA MARGARITA MONTEMAYOR NOGRALES.**

ATTN: MR. EMMANUEL A. ZARATE after the completion of services and submission of required supporting documents to facilitate payment.

X. APPROVED BUDGET FOR THE CONTRACT

The ABC for this project is THREE MILLION FIVE HUNDRED THOUSAND pesos (PhP 3,500,000).