LANDBANK

SERVING THE NATION

SUPPLEMENTAL/BID BULLETIN NO. 1
For LBP-HOBAC-ITB-CS-20221028-01(2)

PROJECT	:	**Enterprise IT Security Risk Assessment**
IMPLEMENTOR	:	**HOBAC Secretariat Unit**
DATE	:	**February 2, 2023**

This Supplemental/Bid Bulletin is issued to modify, amend and/or clarify certain items in the Bid Documents. This shall form an integral part of the Bid Documents.

Modifications, amendments and/or clarifications:

1) The bidder/s are encouraged to use the Bid Securing Declaration as Bid Security.

2) Responses to bidder's queries/clarifications (Annexes I-1 & I-2).

3) The submission and opening of bids is re-scheduled on **February 10, 2023** at 10:00 A.M. through videoconferencing using Microsoft (MS) Teams.

ATTY. HONORIO T. DIAZ, JR.
Head, HOBAC Secretariat Unit

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS

DATE	02 February 2023
PROJECT IDENTIFICATION NO.	ITB-CS-20221028-01(2)
PROJECT NAME	Enterprise IT Security Risk Assessment (EITSRA)
PROPONENT UNIT/TECHNICAL WORKING GROUP	Information Security and Technology Risk Management Department/EITSRA TWG

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS	LANDBANK's RESPONSES
1	3.3.1 – Internal and External VAPT	1. Would want to confirm if the targets are only infrastructure components and not applications.	including applications
2		2. Will it be possible to provide the count and type of the target hosts for the VAPT? -	around 30 internet facing resources, around 270 internal hosts - to be finalized with the winning bidder
3		3. If applications are included, would want to confirm that testing for 3.3.1 would not be part of the SDLC process	no, this activity covers applications in production
4	3.3.2 PCIDSS requirements 3.3.2.1 Penetration Testing	Count and type of the target hosts for the PT?	around 30 hosts/systems
5	3.3.2.2 External Vulnerability Scan	a. What tool will be used?	PCI DSS compliant tool
6		b. Who will provide the tool?	vendor
7	3.3.2.3 Web Application VA	type and # of applications?	6 web apps for retail and corporate customers
8	3.3.2.4 Wireless Access Points	# of locations and # of floors for each location?	by discovery, covering 39 floors (5 sites)
9	3.3.2.5 Segmentation Testing	# of segments and contained hosts for each?	DMZ, Server, User segment- details will be discussed with the winning bidder
10	3.3.2.6 API Assessment	a. # of applications for API testing	10
		b. # of API endpoints (a point at which an API -- the code that allows two software programs to communicate with each other -- connects with the software program) of each application.	Around 35 endpoints
11	3.3.2.7 Mobile Application testing	a. # of application	6 mobile applications (Android and iOS)

ANNEX I-1

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND/OR SUGGESTIONS	LANDBANK's RESPONSES
12		b. Are all applications running on both Android and iOS.	Yes
13	3.3.2.8 ATM/CDM	Are we allowed to bring the ATM offline?	No
14	3.3.4 Security Testing of Web and Mobile Applications	1. # of applications for each test? (e.g.: 2 tests with no more than 1 app for each test)	maximum of 2 applications, with retests after each remediation, retest for various VA fixes is not limited
15		2. Are applications running on both iOS and Android? -	Yes for mobile applications
16		3. Do we have access to their repository?	No. You may perform decompilation as needed or use tools to scan binary.
17		4. Do we have access to your SDLC Pipeline?	No. We do not have automated SDLC pipeline
18		5. Do you have an existing tools for DAST and SAST? (e.g. checkmarx)	Currently, we do not have DAST and SAST
19		6. Do you have an existing list of security requirements?	Yes
20		7. How long is one development life cycle?	Depends on the size of the project, at the average, 1 year after contract signing
21		8. Where will the applications be hosted? (e.g.: dev,test or production)	Development, Test, and Production
22		9. Will full VAPT be involved in this testing at the end of the application's Dev cycle?	Yes
23	**3.3.5** SWIFT Mandated Assessment	1. Is the DR site also following A2 architecture?	Yes
24		2. Will you be able to provide counts to the SWIFT devices identified here?	Yes, covering 6 servers and 13 workstations
25		3. What would be the covered period for the SWIFT scope, 2022 or 2023?	2022, for confirmation with SWIFT
26		4. What version of the SWIFT CSF will be used in the project? Will it cover CSF2022 or CSF2023.	CSCF 2022, for confirmation with SWIFT
27		5. What is the target timeline (start and completion date) for the SWIFT scope?	Start and completion would be the soonest possible time, for discussion with winning bidder
28		6. Is the identified scope items under 3.3.5.3 part of the standard swift control or additional configuration testing outside of the CSF requirements?	part of the CSCF controls validation

ANNEX I - 2