

**BIDS AND AWARDS COMMITTEE
FOR INFORMATION TECHNOLOGY (IT) PROJECTS**

BID BULLETIN NO. 1

This Bid Bulletin is issued to amend/clarify items in the Bidding Documents for the **SUBSCRIPTION TO SECURITY AWARENESS PLATFORM WITH PHISHING SIMULATION AND TRAINING CAMPAIGN**, under **Competitive Bidding No. 2026-10**.

I. CLARIFICATIONS

A. CLARIFICATIONS FROM CREATIVE INFOSOLUTIONS, INC.¹

REFERENCE	CLARIFICATION	RESPONSE
Section VII. Technical Specifications <i>Page 66</i> Access, Set-up, and Configuration	1. For the requirement "phishing simulation websites must be configurable to redirect or land on a domain name designated by the SEC (e.g., look-alike domains) for use in simulation exercises. The supplier shall assist in the configuration, onboarding, and management of these domains for simulation activities", how many customized domains are needed for this?	At least three (3) and should be operational for a period of one (1) year.
Section VII. Technical Specifications <i>Page 69</i> Minimum Technical Requirements	2. For the requirement "Knowledge Transfer Session: To be given to at least ten (10) ICTD Personnel" under Technical Handoff, does SEC prefer classroom type for the 10 personnel ?	Classroom type, face-to-face training, for two (2) batches.

B. CLARIFICATIONS FROM INFOBAHN COMMUNICATIONS, INC.²

REFERENCE	CLARIFICATION	RESPONSE
Section VII. Technical Specifications <i>Page 65-70</i>	3. Could the project proponent provide more details on the process for designating and integrating custom domains for phishing simulations, including technical requirements and lead times?	Prior to the issuance of the certificate of acceptance, the platform shall be capable of identifying and designating custom domains to be used for phishing simulation activities. The deceptive, look-alike, or imposter domain names shall be identified and provided by the SEC, and may closely resemble the organization's legitimate domains (e.g., sec.com.ph) for the purpose of creating realistic

¹ Received on 21 May 2026

² Received on 22 May 2026

		and controlled phishing simulation scenarios as part of cybersecurity awareness exercises. The vendor shall ensure that the custom phishing simulation domains are properly integrated and configured within the platform. The designated domain subscriptions and usage shall remain valid and operational for a period of one (1) year.
	4. Regarding training campaign customization, are there specific themes, content types, or regulatory topics the SEC prioritizes for custom content curation?	The SEC prioritizes the availability and customization of basic and core cybersecurity awareness training materials and campaigns relevant to the organization's operational and regulatory environment. These may include, but are not limited to, phishing awareness, email security, password security and multi-factor authentication (MFA), social engineering, ransomware awareness, safe internet and browsing practices, data privacy and protection, mobile device security, incident reporting procedures, and secure remote working practices.
	5. What specific metrics or parameters does the SEC consider most critical for evaluating human and organizational risk scoring?	Metrics and parameters may include, but are not limited to, training completion rates, assessment and quiz results, simulated phishing campaign participation and outcomes, and reporting of suspicious emails. The SEC also considers overall organizational trends such as department risk levels, phishing success rates, campaign effectiveness, repeated risky behavior, and changes in user awareness over time.
	6. What are the preferred technical protocols or APIs for integration with SEC email systems (e.g., SMTP, API-based for M365/Google)?	The platform should support seamless and ready integration with SEC's existing email environment which is Google Workspace.
	7. What is the expected frequency or criteria for updating vendor-owned proprietary security awareness training courses?	Monthly

	8. Is the Knowledge Transfer Session: To be given to at least ten (10) ICTD Personnel can be conducted on a virtual setup?	Classroom type, face-to-face training, for two (2) batches.
--	--	---

C. CLARIFICATIONS FROM INNOVE COMMUNICATIONS, INC.³

REFERENCE	CLARIFICATION	RESPONSE
Section VIII. Philippine Bidding Document Related Forms	9. May we respectfully submit this clarification to present to you how our Secretary Certificate is structured where we have an Authorized Representative who is authorized to sign all bid related documents, and an Authorized Signatory who is authorized to sign all ensuing contracts. Please see attached cover sheet clarifying the distinction between our Authorized Representative and Authorized Signatories and providing a clear understanding of why our Authorized Signatory is required to sign the Omnibus Sworn Statement.	Noted
	10. May we please confirm if we are required to sign each page of the bidding documents?	Please refer to ITB Clause 17 on page 30 for the instructions on the signing of bids.
	11. May we please confirm if we are required to provide supporting documents (contracts, PO, NOA, NTP, etc) for the list of all ongoing contracts?	Attachment of said documents is not required for the Statement of All Ongoing Contracts. However, complete contact details of point persons for purposes of validation should be included in the Statement.
	12. May we respectfully request this clarification to determine whether the evaluation and award for this procurement will be based on the Lowest Calculated Bid (LCB) or the Lowest Calculated Responsive Bid (LCRB), as this will guide our compliance and bid submission.	As mentioned during the pre-bid conference, Lowest Calculated Bid shall be used as the award criterion for this Project.
Section VII. Technical Specifications	13. Under real-time tracking, what kind of "user behavior"	Under real-time tracking, the platform is expected to monitor

³ Received on 22 May 2026

<i>Page 67</i> Real-Time Tracking	is the platform required to monitor?	user interactions and behaviors related to phishing simulation and cybersecurity awareness activities, including users who opened phishing emails, clicked embedded links, downloaded attachments, submitted credentials, ignored emails, or reported phishing emails in real time. The platform should also provide visibility into user participation, campaign engagement, training completion, and recurring risky behaviors to support the continuous improvement of the organization's cybersecurity awareness posture.
Section VII. Technical Specifications <i>Page 67</i> Security Awareness Training, Quiz, and Assessment	14. Under creation of customised training campaigns, does this include creation of training modules from scratch in the platform?	Preferably, yes. The SEC should also be able to create customized training modules within the platform from scratch, allowing flexibility in designing training content, scenarios, and assessments based on its specific cybersecurity awareness needs and requirements.

Provisions in the bidding documents that are in conflict with this Bulletin are deemed revised/amended. For guidance and information of all concerned.

25 May 2026

For the Bids and Awards Committee:


OLIVER O. LEONARDO
Chairman 