Consultants sought for two S.Korea-backed projects

THE Department of Public Works and Highways (DPWH) said it is inviting consultants to bid for the South Korea-backed feasibility study component of two road projects in Pampanga and Bukidnon.

The department published in a newspaper over the weekend a "request for expressions of interest" for consulting services for the feasibility study of Lubao-Guagua-Sasmuan-Minalin-Santo Tomas Bypass Road, funded by the Philippines-Korea Project Preparation Facility or PK-PPF.

The project will allow motorists from Bataan to bypass congested town centers through to the Santo Tomas section of MacArthur Highway.

The DPWH is requesting similar expressions of interest for consulting services for the feasibility study of the Mount Kitanglad Range Belt Road in Bukidnon.

The DPWH said the documents for both contract packages must be received by the Bids and Awards Committee Secretariat on or before 9 a.m. on March 7.

The Department of Finance (DoF) announced in 2020 that South Korea will provide the Philippines a $50-million loan to fund the feasibility studies and other project preparation activities "necessary to speed up the implementation of the Duterte administration's 'Build, Build, Build' infrastructure projects."

The DoF and the Export-Import Bank of Korea (KEXIM) signed the loan agreement worth to P2.73 billion for the PK-PPF.

"This project preparation facility will have a total cost of about $71 million, of which $50 million will be accessed through the loan extended by KEXIM through South Korea's Economic Development Cooperation Fund (EDCF)," the DoF said.

The balance will consist of Philippine counterpart funding.

"Aside from being a zero-interest loan, KEXIM granted the Philippines a repayment period of 40 years, inclusive of a 10-year grace period," the DoF noted. — **Arjay L. Balinbin**

EU withdrawal of GSP+ privilege not seen derailing PHL recovery

By Revin Mikhael D. Ochave
Reporter

THE LOSS of preferential market access to the European Union (EU) via its Generalized Scheme of Preferences Plus (GSP+) scheme is not expected to deal a major setback to the Philippine economic recovery, economists said.

University of Asia and the Pacific Senior Economist Cid L. Terosa said in an e-mail interview that the Philippines has the sovereign right to manage its internal affairs without external intervention or pressure.

"The EU is an important trade and economic partner, but the Philippines has other partners that do not share EU's point of view. I don't believe that EU by itself can derail the impending economic resurgence of the country," Mr. Terosa said.

The EU requires GSP+ beneficiaries to sign on to various core international conventions regulating worker rights, illegal fishing, and environmental protection. Occasional disagreements over the government's human rights record have led to threats that the Philippines might be denied GSP+ market access.

"For several years now, domestic forces have driven the economy forward and cushioned the impact of external fluctuations on the Philippine economy. External forces have played second fiddle to the power of the domestic market," he added.

On Feb. 17, the European Parliament approved a resolution that called on the Philippine government to address violence and human rights violations or risk temporarily losing access to GSP+ trading arrangements.

The resolution also urged the Philippine government to amend Republic Act No. 11479, or the Anti-Terrorism Act and its implementing rules and regulations, to meet international standards on counter-terrorism.

"I wouldn't say it will stall our economic recovery but it would reduce our exports and lower our investment prospects," Foundation for Economic Freedom President Calixto V. Chikiamco said in a mobile phone message.

Trade Secretary Ramon M. Lopez said in a Viber message that the allegations of the EU on human rights are "fake news" and give a false impression of the Philippines.

"While it is not new, their allegations on human rights and lack of press freedom are fake news, and those only give false impressions on the real situation in the Philippines. They should visit our beautiful country," Mr. Lopez said.

"They should ask the Filipinos in their companies or communities. They should also ask the EU citizens (and) the EU business chambers in the country," he added.

GSP+ allows zero-tariff entry of more than 6,200 Philippine products to EU. The benefits of the GSP+ will apply as long as the country complies with 27 conventions. The trade agreement started in January 2014 and is set to end on Dec. 31, 2023.

Mr. Lopez said the Philippines continues to provide updates to the European Commission. A GSP+ monitoring mission is due to evaluate the Philippines at the end of the month.

"This process is more systematic and organized in obtaining accurate information regarding the real situation in the country. They get to visit as well the projects and the marginalized sectors that get to benefit from the EU GSP+ and other stakeholders," Mr. Lopez said.

In a statement on Sunday, the Department of Trade and Industry (DTI) said an existing dialogue mechanism allows discussion and clarification of the human rights situation and other concerns.

"The Philippines has been very cooperative with the EU and has repeatedly addressed these concerns in existing dialogue mechanisms. The Philippines remains compliant with the 27 international core conventions on human rights, labor, environment and good governance to enjoy GSP+ treatment," Mr. Lopez said.

Mr. Lopez also said that GSP+ helps micro, small, and medium enterprises, fisherfolk, farmers, and workers in the export value chain.

According to Trade Assistant Secretary Allan B. Gepty, the Philippines is willing to work with the EU to address its concerns.

"This is not the first time that the European Parliament approved such a resolution. The European Parliament also passed similar resolutions in 2016, 2017, 2018, and 2020. The Philippine government remains ready to cooperate and work with the EU to clarify these issues and concerns," Mr. Gepty said.

Joseph F. Purugganan, Trade Justice Pilipinas co-convenor, said in a mobile phone message that the Philippine government is solely responsible for drawing scrutiny from the EU.

"We support strongly the demand... to initiate withdrawal procedures for GSP+ trade preferences to the Philippines. Our position is that the Duterte government, by failing to act on the human rights situation and failure to comply with the obligations under the GSP+ program, has forfeited these preferences. The blame falls squarely on the government," Mr. Purugganan said.

The DTI said exports to the EU under GSP+ were valued at 1.6 billion euros in 2020, for a utilization rate of 75% on eligible exports.

"The scheme benefits several communities such as, but not limited to General Santos, Davao, Cebu, and economic zones located in Laguna, Cavite, and Batangas, where most exporters, taking advantage of the scheme, are located," the DTI said.

Carbon tax revenue potential could be 'false hope'

By Marielle C. Lucenio

THE taxation of carbon emissions is not expected to be of much help in raising revenue to pay down foreign debt, analysts said.

While calling such a tax "laudable, timely... (and) consistent with our international commitments," Tax Lawyer and Certified Public Accountant Kenneth L. Manuel told *BusinessWorld* in an e-mail that the promise of using such revenue to reduce foreign debt levels could be raising "false hope."

Mr. Manuel estimated that a carbon emissions tax will raise the equivalent of 1% of the Bureau of Internal Revenue's (BIR) collections.

"According to 2016 estimates, a carbon tax would give the government P20 billion in revenue. ...Without the carbon tax, the BIR was able to collect P1.9 trillion in taxes in 2020. Hence, the imposition of carbon tax is only expected to generate roughly 1% of collections, and that's just BIR. We have not yet factored in other revenue-generating government agencies such as the Bureau of Customs," he said.

Speculation over new taxes arose over the weekend after Finance Secretary Carlos G. Dominguez III granted an interview with CNBC International TV on Friday. Reports emerging in the wake of the interview cited unnamed sources as saying that the government will be looking at "relatively untaxed" sectors of the economy.

FULL STORY
Read the full story by scanning the QR code with your smartphone or by typing the link **<bit.ly/CarbonTax022122>**

Coconut water firm sending trial shipment to China customer

A COMPANY exporting organic coconut products is sending a trial shipment of young coconut to China soon to meet growing demand, estimated at up to 300 40-foot containers monthly, according to the Department of Agriculture-Davao (DA-11) regional office.

The regional office's marketing assistance team recently facilitated a meeting between a group of Chinese buyers and Cocowild Philippines, Inc. for the supply of young coconut, which is the source of fresh coconut water.

Cocowild representative Geralyn M. Hobrero said the company, based in Polomolok, South Cotabato, currently has two satellite facilities that can package young coconut at a volume of up to 18 container vans.

Ms. Hobrero said with the trial shipment, the company is seeking to verify whether it can comply with Chinese entry standards and the buyer's quality requirements.

Apart from young coconut, the company also exports coconut sugar, coco syrup, and honey-cured vinegar.

Regional Executive Director Abel James I. Monteagudo said the DA agency is ready to provide further assistance to strengthen market linkages.

In 2019, Davao-based Eng Seng Food Products started exporting fresh young coconut to China, but could not meet the volume demand. —**Marifi S. Jara**

OPINION

Shifting to a zero-trust mindset

As the world continues to operate under remotely while grappling with the pandemic, the danger of cyberattack remains a constant threat. The current situation has resulted in people using their own devices and networks to ensure business continuity from anywhere, but these are not as secure as corporate systems and connections, and cybercriminals are not letting these easy opportunities pass.

Data security is more critical than ever, with traditional data protection techniques functioning under a "trust but verify" strategy. This perimeter-driven paradigm entrusts its internal users with unobstructed network access and provides security controls only for external or untrusted networks. However, this introduces the issue of misplaced trust that can lead to the IT landscape of an organization being exposed to vulnerabilities.

SUITS THE *C*-SUITE
JOHN N. PANES

With organizations dramatically accelerating their transformation journey, effective cybersecurity that expands beyond the organizations' territories becomes even more significant — and this is where the concept of zero trust comes in.

Zero trust is a security model based on the principle of maintaining strict access controls without trusting anyone by default, including internal users. Everyone is trusted by default in a traditional IT network, and once an attacker gets inside the network, they are free to move and gain access to protected customer data, intellectual property, or network controls. Zero-trust application security understands that attackers can be present both within and outside of a network, which is why zero-trust policy enforcement dictates that no user should be trusted automatically.

With effective zero-trust frameworks in place, organizations can enforce several critical steps as part of their arsenal to reduce cyber risk while establishing access and identity controls.

THE NEED TO ADAPT ZERO TRUST

Newer organizations are now adapting this model as it requires a simpler approach but at the same time yields ever stronger security controls.

The "trust but verify" strategy is no longer an option as targeted, more advanced threats are now capable of moving inside the corporate perimeter. Because of the nature of remote working, accessing applications from multiple devices outside of the business perimeter has become even more prolific. This results in the increasing risk of exposure to data breaches, malware and ransomware attacks.

The zero-trust paradigm requires organizations to continuously analyze and evaluate the risks that involve their business functions and internal IT assets, then form strategies to mitigate them. The zero-trust model also restricts access by only providing access to users who need it while depending on whether they successfully authenticate each access request. The purpose of this process is to help eliminate unauthorized access to services and data while employing a positive security enforcement model. Because it uses a different lens to view data protection, the zero-trust model allows certain criteria that govern access and restrictions.

STEPS TO START THE ZERO-TRUST JOURNEY

The looming challenge for these organizations actually involves where to start. They can begin their zero-trust journey with three simple steps, starting with building a zero-trust center of excellence. This entails creating a cross-functional working group of all the teams that will be working together on a zero-trust architecture. This includes cybersecurity and IT teams that will handle actual deployment, as well as business leaders who will help define the necessary business objectives to ensure successful implementation.

Second, the center of excellence will need to engage in workshops to ensure that everyone is aligned and understands the basic concepts of this model, the business objectives of the organization, and what to protect — data, applications, assets, and services (DAAS). The prototype zero-trust network can be planned during the workshop to allow IT and security practitioners in the organization to better move to a more formal design phase.

Third, start with something low-risk, instead of proceeding ahead with the "crown jewels" of the organization. Deploy zero trust first in an environment where implementation teams can get hands-on experience and develop confidence as they build this simpler but more secure network.

MAXIMIZING DATA SECURITY WITH ZERO TRUST

While there are many misconceptions surrounding the zero-trust architecture model, from its overall functionality to implementation, organizations can focus on five major aspects identified by Murali Rao, EY India Cybersecurity Consulting Leader, to better maximize their data security.

Prioritize top risks. Organizations must understand the attack surface and threat landscape to qualify risks, before prioritizing the ones that will need the most focus.

Enterprise-wide policy. Organizations will need to set policies according to the sensitivity of services, assets and data housed. The potential of zero-trust architecture relies on the access policies that organizations define.

More granular network enforcement. Organizations must always assume that the network is hostile, and that they cannot trust any user or incident. This will mean removing implicit trust from the network and building trust into devices and services.

Implement the zero-trust network based on an inside-out view. Organizations need to include zero-trust architecture as part of their overall transformation strategy. They will also need to implement technologies that help achieve zero trust as their transformation moves them more to the cloud and retires old legacy systems.

A strong Identity and Access Management. Organizations need to work on the authentications of their workloads, devices and users. Technologies such as privilege ID management, multifactor authentication, behavioral analytics and file system permissions must be enforced based on defined rules to minimize the compromise of trust.

THE KEY TO SUCCESSFUL ZERO-TRUST ARCHITECTURE ADOPTION

Breaches that result in lost or stolen data cost organizations significant financial and reputational damage. The zero-trust model aids in both simplification and standardization of access control enforcement across an enterprise with improved compliance and the continuity of critical business processes, and it is most effective when integrated across the entire digital IT estate.

In an era where customers, partners and the supplier ecosystem access data and services from literally anywhere, applying a zero-trust model reduces the risks of security issues that arise due to how organizations often lean on perimeter-based approaches.

This article is for general information only and is not a substitute for professional advice where the facts and circumstances warrant. The views and opinions expressed above are those of the author and do not necessarily represent the views of SGV & Co.

JOHN N. PANES is a manager from the Technology Consulting practice of SGV & Co.