Hybrid exclusion from zero-tariff policy meant to spur EV charging station development — BoI

HYBRID vehicles were excluded from zero-tariff treatment because their widespread adoption could delay the development of charging infrastructure for electric vehicles (EVs), the Board of Investments (BoI) said.

Ceferino S. Rodolfo, Trade undersecretary and Board of Investments (BoI) managing head, said:

"We want to develop the infrastructure, the charging stations. The problem with hybrid (vehicles) is that most of them will not need any charging stations," Mr. Rodolfo told reporters last week.

"The charging stations would not be developed if hybrid vehicles (are allowed for import at zero tariffs). Pure EVs... would spur investment in charging stations," he added.

The National Economic and Development Authority (NEDA) Board announced in November that it endorsed the issuance of an executive order (EO) that would lower the most favored nation tariff rates to zero percent on imported completely built-up units of EVs for a five-year period.

The endorsed EO did not include zero tariffs for imported hybrid vehicles.

Once signed by President Ferdinand R. Marcos, Jr., the zero tariffs will cover electric passenger cars, buses, mini-buses, vans, trucks, motorcycles, tricycles, scooters, and bicycles. The current tariff rates for EVs range from 5% to 30%.

According to the NEDA Board, the EO seeks to expand market sources, boost adoption of EVs, and reduce the dependence on imported fuel.

Mr. Rodolfo added that the decision to exclude hybrid vehicles is in line with the government objective of attracting investment in the local production or assembly of EVs.

"Our ultimate goal is for local assembly, the manufacturing of electric vehicles, which will be leveraging our abundance of green metals, which we want to further add value to. Add to that our strength in software development and strength in electronics manufacturing," Mr. Rodolfo said.

Mr. Rodolfo said that the decision not to include hybrid vehicles is still subject to review in the draft EO.

"The decision of the NEDA Board is to provide a review clause. After one year, we will review the coverage of the products in the EO," Mr. Rodolfo said.

Foreign business chambers have urged the government to reconsider the EO and include hybrid in the zero-tariff order. — **Revin Mikhael D. Ochave**

Agriculture industry lobbies for 'mandatory' Maharlika allocation

THE AGRICULTURE industry said it is hoping to capture as much as 30% of the proposed sovereign wealth fund's investable capital, saying that the wealth fund will draw away funding from the farm sector.

Danilo V. Fausto, president of the Philippine Chamber of Agriculture and Food, Inc. (PCAFI), told reporters Friday, "We demand a mandatory Maharlika Investment Fund share for agriculture productivity."

Mr. Fausto said 25 to 30% of any "activity, investment or investable funds" of the MIF should go to agriculture, because Maharlika draws its funding in part from the Land Bank of the Philippines (LANDBANK) and the Development Bank of the Philippines (DBP).

"These are our agricultural banks. I do not see in the Maharlika Investment Fund anything on the agricultural sector. I want to make it mandatory in the law that a portion of that fund should be invested in the agricultural value chain," Mr. Fausto said.

Last week, the House of Representatives approved on third and final reading the Maharlika bill, with 279 legislators voting in the affirmative and six against.

The Maharlika bill, or House Bill (HB) No. 6608, had been certified as urgent by President Ferdinand R. Marcos, Jr.

The bill lists as "allowable investments" foreign currency, metals, fixed-income instruments, domestic and foreign corporate bonds, equities, real estate, infrastructure projects, loans and guarantees, and joint ventures or co-investment projects.

The initial capital of the Maharlika fund will be put up by LANDBANK, the DBP, and Bangko Sentral ng Pilipinas (BSP).

Mr. Fausto noted that the government should focus on agriculture because it will "certainly generate profit."

"If you put it in processing, milling, drying, logistics, it will make money and I suggest it should not be run by the government," Mr. Fausto added.

The proposed MIF also generated backlash after the initial involvement of pension funds in putting up the capital and the designation of the President as chairman of the fund's board.

On Dec. 15, legislators agreed to remove the Government Service Insurance System (GSIS) and Social Security System (SSS) as Maharlika funders. — **Ashley Erika O. Jose**

Moody's Analytics says lack of capital formation recovery a drag on Philippine growth potential

MOODY'S ANALYTICS said that while parts of the Philippine economy have shown signs of recovery, capital formation continues to lag, possibly signifying economic scarring over the medium term.

Moody's Analytics said it now sees the Philippines' medium-term growth potential at 6%, down from 6.6 % previously, due to the delayed recovery in investment to pre-pandemic levels.

"In the midst of the ongoing recovery, gross fixed capital formation (GFCF) has yet to be restored to pre-pandemic levels, contributing to our view that potential growth may have deteriorated to around 6%," Moody's Senior Vice President and Manager Christian de Guzman said to *BusinessWorld*.

The Philippine Statistics Authority (PSA) estimates GFCF at $21.534 billion in the third quarter, well below the $28.279 billion posted in the last pre-pandemic quarter ending December 2019.

The 6% outlook is supported by other signs of recovery, like the 4.5% unemployment rate, which is below the 4.6% rate reported in the quarter ending December 2019.

"Labor market indicators — such as employment and, conversely, unemployment — have largely recovered, mirroring the very healthy rates of growth since the economy accelerated its reopening in late 2021," Mr. De Guzman said

"However, there has been a partial reversal of the pre-pandemic gains in poverty reduction, suggesting that the financial health of a number of households has not been restored," he added.

Moody's Analytics added that this may be in part to to a greater share of workers involved in "elementary occupations," or informal work, compared to the period before 2020.

Moody's Investment Service has said in a report that the duration of pandemic restrictions means large portions of the school-age population were deprived of formal education with inadequate access to computers, broadband internet and other tools needed to facilitate remote learning.

"If not fully addressed, the lack of a significant catch-up in educational outcomes would weigh on the competitiveness of the Philippine economy in relatively high-skilled sectors, such as business process outsourcing," the report said.

"Against this backdrop, higher inflation could further undermine household balance sheets and dampen the outlook for continued employment growth," Mr. De Guzman said.

"The primary driver of economic scarring for the Philippines has been the combination of the deep recession in 2020 on account of one of the longest and strictest containment regimes in the region, and the delayed reopening of the economy. These factors highly impacted consumption, which is still the most important driver of Philippine growth, and investment as mentioned above," Mr. De Guzman told *BusinessWorld*. — **Aaron Michael C. Sy**

BCDA, Singapore agency promote New Clark City to SME investors

THE BASES Conversion and Development Authority (BCDA) and Enterprise Singapore said they promoted New Clark City to investors from the information and communications technology (ICT) and smart city industries.

In a statement over the weekend, the BCDA said that together with Enterprise Singapore, they conducted a second round of business-to-business and industry-focused meetings with urban development leaders in Singapore.

Enterprise Singapore is an arm of the Ministry of Trade and Industry. Its mission is to support Singapore small and medium enterprises (SME) and boost enterprise development.

The companies met by the BCDA and Enterprise Singapore include those involved in ICT, diversified environmental services, engineering, aviation solutions, and smart city technologies.

Some of the New Clark City projects pitched during the meetings include the common ICT infrastructure network, the data center co-location facility project, the New Clark City affordable housing project, the New Clark City estate and facilities management services, and the operations and maintenance of New Clark City's sports facilities.

"As urbanization continues, we at BCDA understand that smart city technologies and public transport solutions are important in realizing a sustainable and inclusive future for New Clark City. We are very fortunate to partner with Enterprise Singapore who helps us forge connections with some of the global urban mobility and smart city leaders," BCDA President and Chief Executive Officer Aileen R. Zosa said.

"Through their expertise and experience, we will be able to embed global best practices not just in New Clark City but across all the infrastructure projects we are developing," she added.

In September, the BCDA and Enterprise Singapore signed a memorandum of a understanding (MoU) on collaboration with regard to investment opportunities in New Clark City, technology exchange, and bilateral promotion of businesses.

"The MoU with Enterprise Singapore enables the BCDA to increase its understanding of emerging technologies and solutions used in urban development via knowledge sharing and awareness building activities. The MoU also facilitates access for Singapore companies and relevant stakeholders interested to partner in the development of New Clark City," the BCDA said. — **Revin Mikhael D. Ochave**

OPINION

Cybersecurity as a board priority

Cybersecurity came to the forefront of critical concerns when companies had to shift to remote working at the height of the pandemic. Businesses continued to accelerate their transformation to address disruption, but many did not consider cybersecurity as part of the decision-making process — likely due to business urgency or oversight. As a result, as much as 73% of Asia-Pacific businesses saw an increase in disruptive attacks, according to the EY Global Security Survey 2021 (GISS), with new vulnerabilities entering the rapidly evolving business environment.

SUITS THE *C*-SUITE
WARREN R. BITUIN

The industrialization of cyberattacks led to an increase in their volume and severity, but Chief Information Security Officers (CISOs) are faced with challenges that inhibit the cybersecurity function. These include inadequate budgets, which can be seen in the cyber spend of Asia-Pacific businesses totaling only 0.05% of their annual revenue, according to the GISS. This cost-cutting has severe implications, as the GISS reveals that 41% of businesses in the APAC region expect major breaches that could be anticipated and averted with better investment. There is also a lack of preparedness due to the limited visibility of cyber risk within an organization, coupled with outdated or disparate regulations.

The GISS further shows that CISOs demonstrate a lack of confidence when faced with threat actors. Cybersecurity strikes a fine balance between usability, security and cost, but it is only possible if the board is proactively testing and challenging the existing status quo.

BOARD RESPONSIBILITIES TOWARDS CYBERSECURITY

Board members must review the company organizational structure to ensure that the cyber security function is adequately represented, and should promote systemic resilience and collaboration to account for risks stemming from broader industry connections. They should encourage a continuous analysis of comparative metrics, such that industry-accepted cyber frameworks guide data driven decisions, aligning risk appetite with organizational goals and strategy. It is imperative to understand tomorrow's cyber threats today by proactively investigating emerging threats.

Board directors will have to identify their business-critical systems and data, and how their criticality is assessed. They are responsible for key business risks per local applicable Corporations law requirements. In some jurisdictions such as Oceania, directors are now required to take all reasonable steps to be in a position to "monitor and guide" the company and have information made available to them to exercise their responsibilities.

The board must also determine how effective the controls protecting their critical systems and data are, and how often these are tested. In addition, they have to be aware of how their current data privacy and data retention policies align with government and industry regulations, and how third-party suppliers are protecting the company systems and data. Moreover, cyber investments must be focused on mitigating the risk scenarios that the company would be most exposed to. In case of a cyber incident, there has to be an organization-wide response plan capable of addressing it, where employees understand their roles in managing the crisis.

It is the responsibility of directors to consider proactive management of the risks associated with critical assets and data to maintain market and consumer trust, as well as adhering to legislative obligations or best practice expectations to secure personal information.

Thus, it is important to hear from external sources, not just management, about the potential threats and the independent assessed level of controls currently in place. While management can provide updates on the status of the company's cybersecurity programs, an independent party can help the board gain assurance that the programs are adequate with respect to the existing cyber threats that the company is facing.

CYBERSECURITY INSIGHTS FOR BOARDS TO CONSIDER

According to the EY Global Risk Survey (2020), boards stay updated through external advisors or industry analysts (40%), interactions with or data on peer companies (32%), and through management briefings (20%). Almost half of the surveyed respondents consider unfavorable economic conditions, cyber incidents and the pace of technology change to be their top risks.

In light of this, there are several insights gleaned through director dialogues held through the survey. One is to set the cultural tone — boards must demonstrate that cybersecurity and privacy risk are critical business issues by increasing the board and/or committee's time and effort spent discussing the topic. They must also stay updated by increasing the frequency of board and/or committee updates on specific actions to address new cybersecurity and privacy issues and threats.

Moreover, boards must understand the necessary protocols. They have to obtain a thorough understanding of the cybersecurity incident and breach escalation process and protocols, including a defined communication plan for when the board should be notified. By understanding the processes of management to identify, assess and manage the risk associated with service providers and supply chains, they can better manage third party risk. Boards also have to test response and recovery by enhancing enterprise resilience and having the company's ability to respond and recover tested through simulations and arranging protocols with third-party professionals before a crisis. Lastly, boards must monitor evolving practices. They should stay attuned to evolving board and committee cybersecurity oversight practices and disclosures, including benchmarking against peer disclosures for the last two to three years.

SUCCESSFUL AND SECURE TRANSFORMATION

Boards must have a clear understanding of the company's cybersecurity program and how they are effectively implemented to address immediate and near-term cyber threats. Fortifying cyber resilience requires boards to act decisively as major pressures threaten the ability of cybersecurity to effectively address potential risks. They must play an active role in bringing cybersecurity to the rest of the business. By taking more time to discuss cybersecurity risks, the board can send a clear message that the cybersecurity function is a strategic business partner, and that the risks involved are critical business issues. Not only will this help the cybersecurity function work more effectively with the business, but it will also help the function execute transformation programs that are successful and cyber secure.

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

WARREN R. BITUIN is the Technology Consulting Leader of SGV & Co.