Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

EIGHTEENTH CONGRESS
Third Regular Session

HOUSE RES. NO. **2436**

Introduced by Hon. Elpidio F. Barzaga, Jr.

RESOLUTION INVESTIGATING THE ALLEGED DATA HACKING OF THE COMELEC, THE PRESENT AUTOMATED ELECTION SYSTEM, EVALUATING ITS STRENGTHS, VULNERABILITIES AND ACCURACY TO ENSURE INTEGRITY OF THE ELECTORAL PROCESS

WHEREAS, Philippine laws particularly **Articles III, V and XIII of *The Constitution of the Philippines*** guarantee the protection of the Filipinos' basic rights as universal and equal as expression, assembly, freedom of movement, access to courts of law, due process; right to suffrage and secrecy of the ballot.

WHEREAS, at present, multiple laws govern the conduct of Philippine elections, ***The Omnibus Election Code of the Philippines*** **(Batas Pambansa Bilang 881),** amendments and other related laws and regulations thereto such as ***An Act Providing for Synchronized National and Local Elections and for Electoral Reforms, Authorizing Appropriations Therefor, and for Other Purposes*** **(Republic Act 7166)**; ***An Act Authorizing the Commission on Elections to Conduct a Nationwide Demonstration of a Computerized Election System and Pilot-Test It in the March 1996 Elections in the Autonomous Region in Muslim Mindanao and for Other Purposes*** **(Republic Act 8046)**; ***An Act Authorizing the Commission on Elections to Use an Automated Election System in the May 11, 1998, National or Local Elections and in Subsequent National or Local Electoral Exercises, Providing Funds Therefor and for Other Purposes*** **(Republic Act 8436)**; ***An Act Amending Republic Act No. 8436*** **(Republic Act 9006)**; and ***An Act Amending Republic Act No. 8436, Batas Pambansa Bilang 881, Republic Act 7166 and Other Related Election Laws, Providing Funds Therefor and for Other Purposes*** **(Republic Act 9369)**; ***Rules and Regulations on the Resumption of the System of Continuing Registration of Voters*** **(Commission on Elections Resolution No. 190549, 18 July 2019)**.

WHEREAS, the need for an automated election system was necessary in response to increase public confidence and fears of electoral corruption.

WHEREAS, despite concerns and challenges in the move toward automation, public confidence has increased in the automated electoral system.

WHEREAS, on 10 January 2022, the Manila Bulletin has posted a disturbing news article entitled, "Comelec servers hacked; Downloaded data may include information that could affect 2022 elections" stating that, to wit:

"Sensitive voter information may have been compromised after a group of hackers was allegedly able to breach the servers of the Commission on Elections (Comelec), downloading more than 60 gigabytes of data that could affect the May 2022 elections.

This was discovered by the Manila Bulletin (MB) Technews team, which found that the hackers' group managed to breach the system of the Comelec last Saturday, Jan. 8, 2022, and download files that included, among others, usernames and PINS of vote-counting machines (VCM).

The MB Technews team immediately informed Comelec Spokesperson James Jimenez of its findings. Jimenez said he would bring the information to the attention of the Comelec Steering Committee.

In a call to MBTechnews Monday, Jan. 10, 2022, Jimenez said he has yet to get a reply from the Comelec Steering Committee.

The other downloaded files were network diagrams, IP addresses, list of all privileged users, domain admin credentials, list of all passwords and domain policies, access to the ballot handling dashboard, and QR code captures of the bureau of canvassers with login and password.

'Sensitive data downloaded also included list of overseas absentee voters, location of all voting precincts with details of board of canvassers, all configuration list of the database, and list of all user accounts of Comelec personnel,' said MBTechnews.

A source contacted MBTechnews last Saturday, Jan. 8, 2022, to provide information that there was an ongoing hack of Comelec servers.

MBTechnews promptly verified this information, and found that there was, indeed, an ongoing hacking of the servers. Further investigation showed the extent of the hacking to include the Comelec information that were stolen by the hackers."

WHEREAS, in another Manila Bulletin news report dated 10 January 2022, it stated that the COMELEC is already validating the truth of the hacking incident, to wit:

"The Comelec is presently validating the allegations of the article published by the Manila Bulletin, specifically whether Comelec systems have, in fact been compromised," Comelec Spokesperson James Jimenez said in a statement.

With no independent verification that a hack has indeed taken place, one thing immediately stands out: the article alleges that the hackers were able to 'download files that included, among others, usernames and PINS of vote-counting machines (VCM).' The fact, however, is that such information still does not exist in Comelec systems simply because the configuration files – which includes usernames and PINs – have not yet

been completed. This calls into question the veracity of the hacking claim,' he added.

As for the rest of the allegations, Jimenez said, the article offers scant substantiation for its assertions despite claiming that the authors had "verified that there was an ongoing hack."

'Indeed, the article does not even offer proof of such verification,' he said.

The Comelec assured the public of its full and scrupulous compliance with the Data Privacy Act, as well as its continuing cooperation with the National Privacy Commission.

Jimenez said the Comelec will continue its efforts to validate the assertions made by article.

'In this regard, we invite the authors to shed light on their allegations, particularly with regard to the 'verification' they claim to have carried out,' he said.

"Considering that 'news' like this could potentially damage the credibility of the elections, the Comelec stands ready to pursue all available remedies against those who, either deliberately or otherwise, undermine the integrity of the electoral process," added Jimenez.

WHEREAS, in a Manila Bulletin news article dated 11 January 2022, the COMELEC stated that a final report on alleged hacking shall be released this week, to wit:

"The Commission on Elections (Comelec) will release this week the final report on the alleged hacking of their servers.

'Before the week ends we will release a final report on that because the meeting with all our different units will only start this morning,' Comelec Spokesperson James Jimenez told Teleradyo on Tuesday, Jan. 11.

He said the validation is still ongoing.

'We want to know if there really is a data breach. We don't see any evidence of data breach,' said Jimenez.

On Monday, the poll official said they are already validating the allegations of the article published by the Manila Bulletin, specifically whether Comelec systems have, in fact been compromised.

'The article alleges that the hackers were able to 'download files that included, among others, usernames and PINS of vote-counting machines (VCM).' The fact, however, is that such information still does not exist in Comelec systems simply because the configuration files – which includes usernames and PINs – have not yet been completed. This calls into question the veracity of the hacking claim,' Jimenez said.

He said its also important for the poll body to verify such report.

'When you say data breach in Comelec, people will really get nervous. That's why it is important to us that we validate it and in case the report is wrong, of course someone will be responsible for that … because all of a sudden they issue a report without verification,' said Jimenez.

WHEREAS, the Palace and presidential aspirants, Leni Robredo, Bongbong Marcos, Manny Pacquiao and other stake holders have expressed their concerns on the alleged data hacking incident.

WHEREAS, as early as 2016, in a 07 April 2016 article posted by Trend Micro, it stated therein the COMELEC data hacking and data securities issues, to wit:

"Every registered voter in the Philippines is now susceptible to fraud and other risks after a massive data breach leaked the entire database of the Philippines' Commission on Elections (COMELEC). While initial reports have downplayed the impact of the leak, our investigations showed a huge number of sensitive personally identifiable (PII) – including passport information and fingerprint data – were included in the data dump.

Following the defacement of the COMELEC website on March 27 by a hacker group, a second hacker group posted COMELEC's entire database online. Within the day, they added three more mirror links where the database could be downloaded. With 55 million registered votes in the Philippines, this leak may turn out as one of the biggest government-related data breaches in history, surpassing the Office of Personnel Management (OPM) hack last 2015 that leaked PII, including fingerprints and social security numbers (SSN) of 20 million US citizens.

x x x

In a statement, COMELEC spokesperson James Jimenez admits that the security of the website is not high. However, he pointed out that the AVS ran on a different, more secure network and that the recent hack will not affect the machines. Jimenez is confident of the security features of the AVS and reassures involved publics (sic) that things will go smoothly during the elections.

There are, however, discrepancies in the statements made and out findings. COMELEC officials claimed that there were no sensitive information stored in the database. However, our research showed that massive records of PII, including fingerprints data were leaked, included in the data COMELEC deemed public was a list of COMELEC officials that have admin accounts.

"VOTESOBTAINED"

Based on our investigation, the data dumps include 1.3 million records of overseas Filipino voters, which included passport numbers and expiry dates. What is alarming is that this crucial data is just in plain text and accessible

to everyone. Interestingly, we also found a whopping 15.8 million record of fingerprints and a list of people running for office since the 2010 elections.

In addition, among the data leaked were files on all candidates running on the election with the filename *VOTESOBTAINED*. Based on the filename, it reflects the number of votes obtained by the candidate. Currently, all *VOTESOBTAINED*file are set to have NULL as figure.

The COMELEC website also shows real time ballot count during the actual elections. While COMELEC claims that this function will be done using a different website, we can only speculate if actual data will be placed here during the elections and if tampering with the data would affect the ballot count.

Every registered citizen at risk

Regardless whether the hacking could affect the elections, there is still the issue of all voter information that was leaked. Reports stated that while some of the data were encrypted, there were some fields that were left wide open.

Cybercriminals can choose from a wide range of activities to use the information gathered from the data breach to perform acts of extortion. In previous cases of data breach, stolen data has been used to access bank accounts, gather further information about specific persons, used as leverage for spear phishing emails or BEC schemes, blackmail or extortion, and much more.

Data Classification and defending against data breaches

Data breach incidents make daily headlines and affects businesses (whether enterprises or small and medium-sized businesses) from various industries and large organizations. According to our research paper, Follow the Data: Dissecting Data Breaches and Debunking Myths government agencies are the third biggest sector affected by data breach, followed by retail and financial industries. Healthcare and education are the top and second-most affected industries, respectively.

The recent security incidents highlighted the need for stronger security mindset and data classification, given the possible impact of the breach to voters. This also brings to the fore the importance of having data protection officers that would be responsible for the legal requirements as well as securing all types of crown jewels or highly sensitive data of organizations.

'It will be crucial for companies to employ Data Protection Officers, but even then it will be an uphill battle for various reasons, including cultural differences. For example, In Germany, having a Data Protection Officers is necessary by law, but in other countries, it's not. Companies might even think that they don't need one," shares Raimund Genes, Chief Technology Officer for Trend Micro.

Organizations and companies take a heavy hit with each case of data breach, but those who are truly at risk are the owners of the stolen data. As such, instilling a security mindset should be essential when dealing with important data. In the case of COMELEC, companies and organizations should practice data classification. Data classification is done to segregate data of varying sensitivity and applying appropriate protection to each category:

- High Sensitivity – Data such as voter database falls under high sensitivity data, which are confidential and restricted. High sensitivity data, when stolen, may cause damage or harm to one or more individuals.
- Medium Sensitivity – this data is usually for internal public only. The COMELEC leak does not appear to have leaked medium sensitivity data, but examples of which include company emails and documents.
- Low Sensitivity – these data are usually made public and unrestricted. In the leak, low sensitivity data includes the candidate list and their information. Loss of this data type is not considered critical.
- After classifying the data, the next step is to defend them. Methods vary depending on the data, how it's stored, and who can access it. Sensitive data needs to be stored in a separate or disconnected network and needs higher security clearance to be accessed.

Here are other ways to prevent and defend against data breaches:

- Patching systems and network accordingly – regular patching and updating of systems can prevent cybercriminals from exploiting vulnerabilities which can open the doors to your networks.
- Educate and enforce – employees must be trained to respond to threats, know social engineering tactics, and know how to enforce guidelines on how to handle specific situations.
- Implement security measures – create processes that can identify and address network threats. Regularly conduct security audits to make sure all systems connected to the network are secured.
- Create contingencies – in case of a data breach, an appropriate response plan must be put into action. This is to minimize confusion by being ready with persons to contact, steps to mitigate the damage, and strategies to disclose the incident to relevant publics."

WHEREAS, whether or not the data hacking incidents at the COMELEC are true, the COMELEC should be investigated on its technical capacity as a repository of vital information that affect the security of Filipinos.

WHEREAS, if the data hacking incidents are true, what are its effects on the integrity of our electoral process.

WHEREAS, considering that the switch to an automated electoral process spans a considerable length of time, it should be determined if the COMELEC has addressed challenges related thereto.

NOW THEREFORE, BE IT RESOLVED, as it is hereby resolved to conduct an investigation on the alleged data hacking of the COMELEC, the existing automated

electoral process, evaluating its strengths, vulnerabilities and accuracy to ensure integrity of the electoral process.

HON. ELPIDIO F. BARZAGA, JR.
Representative
Lone District of the City of Dasmariñas, Cavite