BoardEffect: Harmful Site

1.1. On 07 May 2020, Advocate Mpumi Nene, CS received a notification of a harmful site, namely *https://nlcboardeffect*. She was subsequently informed by the CIO, Mr Mothibi Ramusi of the block on her account.

1.2. Mr. Mothibi Ramusi, CIO contacted BoardEffect, on 07 May 2020 to discuss the incident and to log a request (#855504).

1.3. The incident was telephonically reported to the Board Human Capital Social & Ethics Committee, by the CIO, Mr Mothibi Ramusi, on 07 May 2020.

1.4. On 07 May 2020, Mr Mothibi Ramusi, CIO informed Ms. Thabang Mampane, Commissioner, via email, of the incident and the action taken. He informed her that he engaged with both BoardEffect and Mimecast ***"for a deep check on this matter"*** and of the fact that they were investigating the matter. He further informed the Commissioner Ms Thabang Mampane that he would advise her on and Advocate Mpumi Nene, CS on the way forward, after the preliminary checks.

1.5. On 07 May 2020, Advocate Mpumi Nene, CS informed the Client Advocate of BoardEffect, Fozia Yusuf, that the NLC has instituted an independent investigation on the incident **which needed to be resolved within the next 72 hours**.

1.6. NEO Solutions was appointed to provide the following services:

i) Conduct a general cybersecurity controls review;

ii) Conduct a vulnerability assessment and penetration testing; and

iii) Conduct digital forensic investigation.

9

1.7. Mr Mothibi Ramusi, CIO, although being the custodian of information systems, was informed of the independent investigation, by Advocate Mpumi Nene, CS, on 07 May 2020.

1.8. The Commissioner, Ms Thabang Mampane prepared a submission dated "*06 May 2020*", to deviate from normal procurement procedures to appoint NEO Solutions as the preferred service provider to conduct a general cybersecurity controls review, vulnerability assessment, penetration testing and digital forensic investigation into NLC's security systems. The submission was recommended by Mr. Mogoboya Matsebatlela, Senior Manager Supply Chain Management. The CFO, Ms Xolile Ntuli approved the submission on 07 May 2020.

1.9. As background to the submission, the Commissioner, Ms Thabang Mampane argued that the Lottery Industry has very limited space for service providers with industry specific expertise and poses a challenge with procuring knowledgeable experts. She went further stating that sensitive information will be exchanged with service providers in an open bidding process that will compromise the security and integrity of the NLC.

1.10. The supply chain requirements referred to in the submission are:

i) Constitution Section 217: the system must be fair, equitable, transparent, competitive and cost-effective;

ii) Treasury Regulation 16A6.4: provides grounds for dispensing with normal procurement prescripts, but reasons must be recorded and approved; and

iii) Practice Note 8: in urgent or emergency cases, the accounting authority may procure by means of price quotation or negotiations, in accordance with Treasury Regulation 16A6.4.

1.11. According to the proposal the factors as mentioned in the submission "*will be able to pass the muster of emergency procurement circumstances which justify the procurement of experts by the NLC by means of a deviation process in accordance with item 8.3 of Instruction Note 3 of 2016/2017'.*

1.12. According to the Submission the investigation was requested by the Board Human Capital, Social & Ethics Committee. The minutes of the Board Committee is however silent pertaining to the request.

1.13. On 15 May 2020, Ms Mary Lou Leader, Director Customer Services, BoardEffect provided Ms Thabang Mampane, Commissioner, with an update on their investigation into the incident, as performed by their security team. She also informed the Commissioner that their security team will continue to investigate the incident to identify the root cause.

1.14. On 20 August 2020, the Ms Farhana Suder, Group Head Legal, Governance, Human Resources, BoardEffect informed the Commissioner, Ms. Thabang Mampane that their preliminary assessment indicated that *"there are no weaknesses with BoardEffects. The concern emanates from the local set up of the NLC's machines and policies, which are currently in place, which we will be reviewing as part of the General Controls Review".*

1.15. Internal Audit issued a Memorandum dated 28 September 2020, pertaining to the security alert on BoardEffect. Internal Audit found that *"the security incident did not result in exploitation (Hacking) of the identified vulnerability and the .js file was flagged and blocked based on Mimecast URL Protection Definitions configurations/settings.* A recommendation was made that BoardEffect should consider performing a penetration test or external vulnerability assessment.

1.16. Ms Farhana Suder, Group Head Legal, Governance, Human Resources, BoardEffect sent the Commissioner, Ms Thabang Mampane, the following reports as compiled by BoardEffect, based on their investigation and assessment, on 12 and 13 October 2020:

i) Cybersecurity Controls Review Report;

ii) External Penetration Testing and Web Application Assessment Report;
iii) Internal Vulnerability Assessment and Penetration Testing Report; and
iv) Excel Spreadsheet containing all the identified vulnerabilities.

1.17. According to Mr Mothibi Ramusi, CIO, they realised after a day or two that the email was not harmful.

1.18. NEO Solutions submitted an invoice dated 28 September 2020 for R498 000.00. The NLC issued a purchase order dated 27 October 2020, thus after the services were rendered.

1.19. NEO Solutions was paid R498 000,00, only R2 000,00 less than the R500 000,00 threshold. This amount can be deemed as fruitless and wasteful expenditure as Diligent provided the same services at no cost.

BoardEffect: Harmful Incident

1.20. We agree with the AGSA in that the NLC incurred irregular expenditure with the appointment of NEO Solutions, to investigate the incident, as there are several companies within the IT industry and an IT company was already contracted by the NLC for the provision of IT related services.

1.21. If there were a fear that an open bid process would compromise the security and integrity of the NLC, Edge Consulting, an appointed IT Company within the NLC could have been requested to assist with the incident, as their contract made provision for special projects.

1.22. The incident should have been resolved within 72 hours however, NEO Solutions only submitted an invoice for payment, during September 2020. BoardEffect already informed the Commissioner, Ms Thabang Mampane of

the root cause of the incident, on 15 May 2020. Taking into account the scope of work defined in the submission it would have been impossible to conclude the assignment within 72 hours.

1.23. The scope of work, as per the submission did not focus on the incident but rather on security of the NLC's information systems and review of policies and best practice.

1.24. According to the submission, NEO Solutions did provide similar services to the NLC, before. We could however not substantiated any similar services rendered by the company.

1.25. Furthermore, the incident was investigated by BoardEffect, and they provided regular feedback on the progress and findings. Internal Audit also performed a walkthrough on the incident and submitted a report, to management. The reason to deviate from competitive bidding processes, to appoint a service provider can thus be questioned, as information technology experts already commenced with a full-blown investigation, without cost, before the appointment of NEO Solutions.

1.26. The criteria to select and appoint NEO Solutions was not provided, in support of the selection and appointment of the service provider.

1.27. According to Treasury Regulation 16A6.4 the deviation should be approved by the accounting authority. This submission could thus not have been approved by Ms Xolile Ntuli, CFO. It should have been approved by the Board.

1.28. NEO Solutions submitted an invoice for the full amount based on an interim report. It appears as if a final report was not issued, as we could not be provided with a final report.

1.29. Ms Xolile Ntuli, CFO and Ms. Thabang Mampane, Commissioner, contravened the following legislative requirements:

Act/Policy/Procedure/Regulation	Clause/Paragraph
Public Finance Management Act (PFMA) Act 1 of 1999 Definition	"irregular expenditure" means expenditure, other than unauthorised expenditure, incurred in contravention of or that is not in accordance with a requirement of any applicable legislation,
Public Finance Management Act (PFMA) Act 1 of 1999 Definition	"fruitless and wasteful expenditure" means expenditure which was made in vain and would have been avoided had reasonable care been exercised
Public Finance Management Act (PFMA) Act 1 of 1999 Section 57	**Responsibilities of other officials** An official in a public entity – (a) must ensure that the system of financial management and internal control estbablished for that public entity is carried out within the area of responsibility of that official;
Public Finance Management Act (PFMA) Act 1 of 1999 Section 57	**Responsibilities of other officials** An official in a public entity – (b) is responsible for the effective, efficient, economical and transparent use of financial and other resources within that official's area of responsibility;
Public Finance Management Act (PFMA) Act 1 of 1999 Section 57	**Responsibilities of other officials** An official in a public entity – (c) must take effective and appropriate steps to prevent within that official's area of responsibility, any irregular expenditure and fruitless and wasteful expenditure and any under collection of revenue due
Supply Chain Management Policy 7.2 Responsibility of officials	7.2.2 Each official shall take appropriate steps to prevent any unauthorised, irregular and fruitless and wasteful expenditure in their areas of responsibility.
Supply Chain Management Policy 7.2 Responsibility of officials	7.2.7 SCM Practitioners and other role players shall carry out their procurement activities with in their line of responsibility and take appropriate steps to prevent unauthorised, irregular and fruitless and wasteful expenditure, and shall adhere to the provisions of this policy. All SCM personnel and other role players involved in any procurement activities shall conduct themselves inaccordiance with NLC Ethics and Conduct Policy and Treasury Code of Conduct for SCM Practitioners. Any breach of these codes shall lead to disciplinary action being taken against the respective official.
Supply Chain Management Policy 7.10 System of Acquisition Management	**7.15.2 Order processing** 7.15.2.2 Each order shall be appropriate authorised prior to the service being rendered.

Lastly, with regard to NEO Solutions, we note that the AGSA identified discrepancies in relation to the submission for deviation. The said discrepancy relates to the date of the submission for approval being 06 May 2020, whereas the incident forming the basis of deviation is occurred on 07 May 2020. In light of the aforesaid, the NLC should provide an explanation as regards the discrepancy for consideration by the AGSA.

AGSA reviewed the procurement of the services and motivation for the procurement process detailed below:

Service Provider	Nature of Service Provider	Value of Award	Purchase Order Number	Motivation/Rationale for single source procurement (As per submission memo)
NEO Solutions	IT Services and Advisory	R498,000	10642	"NEO-Solutions is **leading firm in business process re-engineering and information technology as well as security and safety.** NEO Solutions has been identified to conduct this assessment/investigation as they have **conducted similar work for the NLC previously**". They will conduct a general cybersecurity control review, conduct a vulnerability assessment and penetration testing and conduct digital forensics investigation.

During review of the information provided, the AGSA noted that the procurement of the above IT and Advisory Services to the value of ***R498,000*** *was not done through a competitive bidding process as required by Par 7.10.4.1 of the SCM policy, but* ***through deviation*** *from normal procurement processes.*

Furthermore, the IT and Advisory Services ***does not meet the requirement for deviation*** *from normal procurement processes due to the following reasons:*

- *Information reviewed shows that there was* ***sufficient time to obtain*** *a minimum of* ***three quotations*** *because the* ***deviation*** *was* ***approved*** *on the* ***07 May 2020****, however the* ***purchase order*** *was* ***only issued on 27 October 2020;*** *and*
- *Interim status report was submitted by NEO Solutions on 28 September 2020 in terms of supporting evidence submitted with the invoice.*

Furthermore, the AGSA identified discrepancies on the supporting documents for this deviation that include the following:

- *The submission supporting the* ***deviation was recommended by the Commissioner on 06 May 2020*** *and* ***approved by the CFO on 07 May 2020****. It was noted that the* ***incident*** *which led to the emergency* ***occurred*** *on the* ***07th of May 2020 per the submission****, the CIO* ***reported in a Board Committee meeting*** *which was* ***held on 07 May 2020*** *that there has been a hacking incident detected.*
- *Furthermore, NEO Solutions* ***purchase order*** *was* ***only approved*** *on* ***27 October 2020,*** *however they already started rendering the services prior to receiving the purchase order as the* ***invoice date (28 September 2020)*** *preceded the purchase order date 27 October 2020.*
- *The AGSA was not provided with the rationale for nominating NEO Solutions as opposed to other service providers.*
- *Furthermore, evidence of the quotation received from NEO Solutions were not furnished to the AGSA.*

The AGSA could also not verify whether NEO Solutions indeed rendered the said services as the ***final report was not provided*** *at the date of this finding. The AGSA was not provided with evidence of the meeting invites and the minutes of Board Committee meeting to verify the exact date on which the submission supporting the deviation was made.*

Based on the supporting evidence submitted for this deviation, NLC had ***sufficient time to invite a minimum of three quotations*** *and the* ***deviation is unjustified.*** *The AGSA therefore concludes that this deviation does not comply with PFMA, National Treasury Instruction Note and the SCM Policy and is therefore irregular. Furthermore, the* ***rendering of services*** *by NEO Solutions* ***prior to receiving the purchase order*** *was in contravention of par. 7.15.2.2 of the SCM policy and is therefore unauthorised expenditure.*

Management Comments:

Management disagrees with the finding.

The National Lotteries Commission (NLC) was established of section 3 of the Lotteries Act no 57 of 1997, as amended. In terms of the PFMA and regulations the NLC is required to conduct a risk assessment to determine the material risks to which the institution may be exposed and to evaluate the strategy for managing these risks.

The NLC's Risk Appetite Framework (RAF) sets out the organisational risk appetite statements and tolerance levels that are aligned to the APP that was approved by the Board. It provides a structured approach for the management, measurement and monitoring process for risks and opportunities within the tolerable limits.

The NLC's risk appetite statements emphasis the Board's intentions and the boundaries within which management is expected to operate when pursuing organisation's strategy.

In the past 4 years the NLC has experienced serious information security breaches causing irreparable harm to the organisation. The NLC, like any other entity is not immune to cyber security threats, and the risk was heightened in the past financial year, with the advent of the Covid-19 pandemic resulting in most operations and in particular, Corporate Governance structure engagements being held on virtual platforms.

The reputational harm caused to the NLC, and potential cyber security threats poses an immediate risk to the intellectual property and operational environment.

On 7 May 2021, during a Board Human Capital Social & Ethical Committee meeting, the CIO interrupted the meeting stating there was an attempt of cyber security breach and the meeting was halted.

The members instructed Commissioner to commission an urgent investigation into the matter. The matter was required to be included within 72 hours from instruction, given the sensitivity of information contained on BoardEffect as well as the fact that the platform is utilised for all Board and Board Committee meetings.

The response to the Breach is aligned to the inherent risk assessed as well as the Board's risk tolerance level detailed below:

Risk(s)	Indicator	Acceptable	Cautionary	Unacceptable	Reporting Frequency
Cyber Security Threats	Percentage of detected and prevented cyber security and information	100% detected and prevented cyber security breach incidents	N/A	<100% detected and prevented cyber security breach incidents	Monthly

Risk(s)	Indicator	Acceptable	Cautionary	Unacceptable	Reporting Frequency
	security incidents				
Information Management security threats	Percentage of unauthorised access/ distribution of sensitive information	0%	0%	>1% incident of information classified as confidential and for internal use published in the media	Quarterly

The National Treasury SCM Instruction No 3 of 2016/2017 paragraph 8.2 prescribes that an emergency procurement may occur when there is a serious and unexpected situation that possess an immediate risk to health, life. property or environment which call an urgency to action and there is insufficient time to invite competitive bids.

Management treated the instruction with urgency and given the need to conclude within 72 hours it was impractical to follow normal procurement process due to the matter being urgent.

The assignment was more complex than anticipated and as a result of the Covid-19 pandemic regulations, the review was protracted in the report provided to the BARC Chairperson in October 2020.

NLC procured on an urgent basis in line with instruction note 3 of 2016/2017 paragraph 8.2.

19.20 Maphosa reported the following pertaining to NEO Solutions:

Report Dated – 23 June 2022 (Exhibit O1)	Report Dated – 18 August 2022 (Exhibit O2)
Analysis 27.15 Neo Solutions was selected to address an apparently urgent IT security issue. However, there are several glaring and dubious inconsistencies, including:	**Analysis** 12.84 Neo Solutions was selected to address an apparently urgent IT security issue. However, there are several glaring inconsistencies, including: 12.84.1 The invoice provided to the NLC has no branding, logo or

Report Dated – 23 June 2022 (Exhibit O1)	Report Dated – 18 August 2022 (Exhibit O2)
17.15.1 The invoice provided to the NLC has no branding, logo or form of identifying the business. 17.15.2 A Windeed search conducted on Neo Solutions (Registration Number 2003/0187707/07 as it appears on the invoice) confirms that one of its current directors is Vivien Natasen. 27.15.3 There are a number of entities that appear to be linked to Neo Solutions. However, none of these companies perform the services required by the NLC. 27.15.4 One of such companies is Neo Africa which provides the following services: 27.15.5.1 Customised application systems for various client requirements. 27.15.5.2 Integrated platforms with hardware and software. 27.15.5.3 Surveillance systems with integrated CCTV, licences plate recognition and biometric technology. 27.15.5.4 Precise vehicle tracking and tracing systems. 27.15.5.5 Advanced radio frequency identification systems 27.15.5.6 Customised facilities and asset management systems. 27.15.5.7 Integrated communication networks using appropriate mix of fixed line and mobile communications. 27.15.5 Another company that forms part of th “Neo Group” is Neo Solutions Security, is a private security company allegedly registered with the Private Security Industry Regulatory Authority (PSIRA). The services rendered by Neo Solutions Security are as follows: 27.15.6.1 protection services; 27.15.6.2 surveillance and counter surveillance 27.15.6.3 security systems; and 27.15.6.4 VIP and executive protection using state of the art technology 27.15.6 Neo Solutions Security’s website claims that they are a leader in electronic security solutions and	form of identifying the business. 12.84.2 A Windeed search conducted on Neo Solutions (Registration number 2003/0187707/07 as it appears on the invoice) confirms that whilst there are a number of entities that appear to be linked to Neo Solutions. However, none of these companies perform the services required by the NLC. 12.85 It is clear from our search/assessment that Neo Technologies also do not, in the ordinary course, offer the services required by the NLC and for which R498 000,00 remitted. 12.86 Given the fact that no supporting documentation was provided to us explaining how the figure of R498 000,00 was made up, we maintain the strong believe that there may be fraudulent or criminal conduct involved in the appointment of Neo Solutions. 12.86.1 The submission supporting the deviation was recommended by the Commissioner on 06 May 2020 and approved by the CFO on 07 May 2020. It was noted that the incident which led to the emergency occurred on the 07th of May 2020 per the submission, the Chief Information Officer reported in a Board Committee meeting which was held on 07 May 2020 that there has been a hacking incident detected; and 12.86.2 Neo Solutions purchase order was only approved on 27 October 2020, however they already started rendering the services prior to receiving the purchase order as the invoice date (28 September 2020) preceded the purchase order date (27 October 2020) 12.87 Whilst there may be some justification for the appointment of the service provider, there appear to be far too many inconsistencies to ignore. 12.88 It would certainly be in the NLC’s interest to consider further investigation of this transaction.

Report Dated – 23 June 2022 (Exhibit O1)	Report Dated – 18 August 2022 (Exhibit O2)
offer biometrics, facial recognition and CCTV surveillance. No reference is made to cyber security threat assessments or investigations. 27.15.7 We can confirm that another company affiliated to Neo Solutions is "Neo Africa Technology" as director search confirms Mr Natasen and Suder Farhana as directors. 27.15.8 Duder Farhana is a former director of Neo Solutions but is an active director of Neo Africa Technologies. 27.15.9 Neo Africa Technologies is also a security company based in the North West. Its service offerings include the following: 27.15.9.1 Security Solutions 27.15.9.2 Consumables; 27.15.9.3 Hardware Services; 27.15.9.4 Software; 27.15.9.5 Enterprise; 27.15.9.6 Managed Print Services; 27.15.9.7 Cloud Solutions; and 27.15.9.8 Technical Services. 27.15.10 It is clear from the above list that Neo Technologies also do not offer the services required by the NLC and for which R498 000.00 remitted. 27.16 Given the fact that no supporting documentation was provided to us explaining how the figure of R498 000.00 was made up and the fact that no final report was generated during the AG's audit, we hold the strong belief that there may be criminal conduct involved in the appointment of Neo Solutions. 27.17 This is further exacerbated by the fact that the director of Neo Solutions Mr Natasen Vivien has appeared before the State Capture Commission on allegations of money laundering. 27.18 This is contrary to Management's reply on the AG's findings is so far it relates to the NLC guarding against reputational harm. The NLC have, under these circumstances and the context of the AG's findings, placed the already fragile reputation at risk by transacting in such manner with Neo Solutions who are alleged to have received millions of rands (approximately R10 million) through less	

Report Dated – 23 June 2022 (Exhibit O1)	Report Dated – 18 August 2022 (Exhibit O2)
than transparent payments by South African Express Airways. 27.19 Whilst no criminal cases have been opened against Neo Solutions, a simple due diligence by the NLC would have revealed the risks of reputational damage associated with conducting business with Neo Solutions. 27.20 We also note that the total amount paid to Neo Solutions this total amount is strangely just below the limit of R500 000.00 which would otherwise require a public bidding tender (BSC based process) as per the NLC SCM policy. 27.21 The difference of R2 000,00 appears to be a deliberate attempt to circumvent the need to seek approval from National Treasury.	
Recommendations 27.22 In light of the above, and given the context of this transaction, we believe that there may be an element of criminal conduct involved and that the NLC should strongly consider reporting the transaction and all employees involved in recommending and approving the transaction to the South African Policy Service for further investigation.	**Recommendation** 12.89 In light of the above, and given the context of this transaction, we believe that there may be an element of criminal conduct involved and that the NLC should consider the transaction for further investigation.

19.14 On 07 May 2020, at 11:11, *Postmaster@nlcsa.org.za* sent Advocate Mpumi Nene, CS the following message "*URL Protect clocked access to a harmful site".* The URL was *https://nlc.boardeffect.com.* Mr Mothibi Ramusi, CIO, subsequently informed Advocate Mpumi Nene of the "block" on her account. (**Exhibit H3.1**)

19.15 Mr Mothibi Ramusi, CIO informed Advocate Mpumi Nene, CS, on 07 May 2020, at 11:17, via email, that he is in contact with BoardEffect and that he will revert back. He requested her to work outside the platform till further notice. Advocate Mpumi Nene responded requesting feedback by 13:00. (**Exhibit H3.1**)

19.16 The *"Support Desk"* of BoardEffect sent an email to the CS, Advocate Mpumi Nene, on 07 May 2020, at 11:37. As per the email: (**Exhibit H3.2**)

... Your request (855504) has been received and is being reviewed by our support staff.

19.17 The Advocate Mpuni Nene, CS responded stating that: *"Your urgent feedback on attempts to log onto NLC account and security report will be appreciated".* Mr Roland Pusker, from the BoardEffect support desk, responded stating: (**Exhibit H3.2**)

It sounds like your organisation may not have our current whitelist information in place. Please forward the following to your CIO.

Please set all local hardware and software to ignore traffic going to and from the BoardEffect servers. Exception rules should be enabled for any web content filtering, network caching or antivirus scanning.

Additionally, BoardEffects send notifications on the user's behalf, therefore, we suggest whitelisting mail originating from boardeffect.com.

19.18 The following was recorded in the minutes of the Board Human Capital Social & Ethics Committee meeting, held on 07 May 2020: (**Exhibit H3.3**)

The CIO dialled-in and advised that he received notification on a malicious email gateway and was concerned about its effect on BoardEffect. He recommended that members log-off BoardEffect and adjourn the meeting pending feedback.

19.19 Mr. Mothibi Ramusi, CIO sent an email to the Commissioner, Ms Thabang Mampane, on 07 May 2020, regarding the investigation of the malicious link. As per the email: (**Exhibit H3.4**)

At 10:00am this morning I received a mail noticed related to harmful site that the CFO was trying to access.

I immediately called the CFO to enquire about the site she wanted to access: she confirmed same as that of BoardEffect.

As CIO and that of being a super administrator, I receive messages and reports of blocked mails and/or sites for our records: this is part of alert checks.

Also of note, any mail that is blocked by the NLCs email security gateway – a reason for that is also furnished.

In this particular case the reason recorded was ***"malicious".*** *Normally this message is aligned to sites that are harmful which must not be ignored if detected.*

Upon receiving that notice – I felt obliged to alert EXCO also having heard that there is HCM Board Committee meeting – members accessing BoardEffect.

I am not privy to how other members may have accessed the BoardEffect, but it was through the link I would have received the notice. Also, if the site can easily be accessed via a shortcut created link, then the behaviour should be the same as that of the link, if not, further checks are necessary.

I immediately asked CS to alert the Chair of the HCM Board Committee to halt the meeting and instructed all members to log out of BoardEffect whilst we investigate the matter at hand.

I have since engaged both with BoardEffect (via CS Office) and Mimecast for a deep check on this matter.

As soon as we are done with our preliminary checks, I will advise CM and CS on the way forward.

***NB:** I have noticed that the BoardEffect access is through a download from their site.*

I can further confirm that I have received similar notices for Marjorie and CS accounts: they both tried to access the site the link from the autoreply notice from BoardEffect.

19.20 On 07 May 2020, Advocate Mpumi Nene, CS sent an email to Fozia Yusuf, BoardEffect Client Advocate, enclosing correspondence from the Commissioner. As per the correspondence: **(Exhibit H3.5)**

We refer to the incident reported to you and on BoardEffect system under reference: BoardEffect – Request Received (#855504) on suspected security breach. The NLC has instituted an ***independent investigation*** *on the incident* ***which we need to resolve within the next 72 hours.***

BoardEffect is requested, as a matter of urgency, to provide a comprehensive security report detailing all log-ins over the past 6 months

and any cyber security threats or attempted threats a report of this nature could contain including IP information from where the system was accessed or attempted to be accessed over the specified period.

We trust the above is in order and look forward to your response by no later than Monday, 11 May 2020.

19.21 Fozia Yusuf, Client Advocate, acknowledge receipt of the letter on 07 May 2020. (**Exhibit H3.5**)

19.22 On 07 May 2020, Advocate Mpumi Nene, CS informed Mr. Mothibi Ramusi, CIO, via email, of the investigation. (**Exhibit H3.5**)

19.23 The **Commissioner**, Ms Thabang Mampane, prepared a **submission dated 06 May 2020**, to **deviate** from procurement process and tender procedures in terms of TR16A6.4, for the appointment of a service provider for ICT assessment and advisory. (**Exhibit H3.6**)

19.24 The submission was **recommended** by Mr. Mogoboya Matsebatlela, Senior Manager Supply Chain Management, on 07 May 2020. The submission was **approved** by Ms Xolile Ntuli, **CFO**, on **07 May 2020**. As per the submission: (**Exhibit H3.6**)

BACKGROUND

...

*It is so that the Lottery industry has a very **limited space of service providers** with **industry specific expertise,** and this therefore **poses a challenge** with regards to **procuring knowledgeable experts**. Moreover, information from a sensitive nature will be exchanged with potential service providers within the*

*context of an **open bid** process. This will invariably **compromise the security and integrity** of the National Lottery.*

Section 217 of the Constitution provides:
*"(1) When an organ of state in the national, provincial or local government, or any other institution identified in national legislation, contract for goods or services, it must do so in accordance with a **system which is fair, equitable, transparent, competitive and cost-effective.**"*

*Treasury Regulation 16A6.4, read together with Practice Note 6 of 2007/2008, Practice Note 8 of 2007/2008 and Instruction Note 3 of 2016/2017, provide for grounds for **dispensing with normal public procurement prescripts**.*

*Practice Note 8 provides that: "Should it be impractical to invite competitive bids for specific procurement e.g., in **urgent or emergency cases or in case of a sole supplier**, the accounting officer/accounting authority may procure the required goods or services by other means, such as price quotations or negotiations in accordance with Treasury Regulation 16A6.4. The **reasons from deviating** from inviting competitive bids should be **recorded and approved** by the accounting officer/accounting authority or his/her delegate. Accounting officers/authorities are required to report within ten (10) working days to the relevant treasury and the Auditor General all cases where goods and services above the value of R1 million (VAT inclusive) were procured in terms of Treasury Regulation 16A6.4. The report must include the description of the goods or services, the name/s of the supplier/s, the amount/s involved and the reasons for dispensing with the prescribed competitive bidding process."*

DISCUSSION

*On **7 May 2020,** the Board Human Capital, Social and Ethics Committee was **interrupted by the CIO,** citing that the **BoardEffect** (meeting platform) utilised for circulation of Board and Board Committee documents classified "secret" in accordance with the NLC's Classification and Information Handling policy was*

compromised ***"Hacked".*** *The members requested that an* ***investigation*** *on NLC's servers* ***be commissioned*** *as a matter of urgency. This led to the* ***security and integrity of information on the NLC's servers being compromised.*** *In order to secure the integrity of the information in the quickest manner possible and avoid further damage, a* ***service provider*** *has to be* ***procured as a matter of urgency*** *to:*

- *Conduct a general cybersecurity controls review.*
- *Conduct a vulnerability assessment and penetration testing.*
- *Conduct digital forensics investigation.*

The scope of work and objective of the service provider's appointment entails conducting a ***high-level assessment*** *which comprises a systematic analysis of the security of the NLC's information system by reviewing and analysing how the NLC's security systems measures against or conforms with best practice benchmarks of established criteria with similar institutes. This includes conducting an assessment of related IT governance enablers including NLC Strategy and Business Requirements, IT Strategy, IT Policies and Procedures identifying the security weakness which may have contributed to the leakage of sensitive information belonging to the NLC.*

NEO Solutions Pty Ltd is a leading consulting firm *in business process re-engineering and* ***information technology*** *and communications as well as* ***security and safety.*** *NEO Solutions Pty Ltd has been identified to conduct this assessment/investigation as* ***they have conducted similar work for the NLC previously****.*

The NLC submits that cumulatively, the above factors will be able to ***pass the muster of emergency procurement circumstances*** *which justify the procurement of experts by the NLC by means of a deviation process in accordance with item 8.3 of Instruction Note 3 of 2016/2017.*

FINANCIAL IMPLICATIONS

The total cost implication will not exceed the amount of ***R500 000.00***

19.25 On 15 May 2020, Ms. Mary Lou Leader, Director Customer Success, BoardEffect sent an email to the Commissioner, Ms Thabang Mampane, informing her of their investigation into the incident. As per the email: **(Exhibit H3.7)**

... this matter has been forwarded to me for follow-up. My outreach today is twofold: First, I'd like to offer my sincere apologies for the tardiness of this update on the status of the incident reported and logged in our system as #855504. There are a number of reasons that caused the lapse, and I regret any frustration this may have caused you. Second, our Security team has provided an update, included below:

> *As of* ***14-MAY*** *The Diligent Security Team in conjunction with Mimecast has been investigating this issue identified by NLC involving the NLC-BoardEffect platform (URL) marked as malicious by Mimecast, The BoardEffect platform URLs contain JavaScripts that execute to render the web page appropriately, this is common practice in web applications. When asked about the particular JavaScript file that was marked malicious, Mimecast responded "JavaScript extensions are blocked in general. The option to Block URLs Containing Dangerous File Extensions under the URL Protections definition is what catches this particular extension.*
>
> *Upon further investigation with Mimecast, it was confirmed that Mimecast is simply marking all URLs with JavaScript extensions as malicious by default. Currently, BoardEffect is unable to quickly change this workflow as it requires extensive change to rendering workflow and development.*

Please note, the warning will only appear if the user clicks the link through an email. It will not cause an issue if they manually navigate to the webpage. Lastly, should NLC wish to review recent login reports to their BoardEffect Platform a Customer Administrator of the NLC BoardEffect Platform is advised to log into the platform, navigate to Settings in the upper right corner, and then selecting Reports.

The Diligent Security Team is continuing to investigate the identified issue and will provide an update accordingly.

Going forward, I will provide updates on the status of the investigation. …

19.26 On 20 August 2020, Ms. Farhana Suder, Group Head Legal, Governance, Human Resources, BoardEffect informed, the Commissioner Ms Thabang Mampane, that: (**Exhibit H3.8**)

With regards to the assessment conducted to determine the security integrity of BoardEffects, please be advised that our ***preliminary assessment indicates*** *that there are* ***no weaknesses with BoardEffects****. The concern emanates from the local side* ***set up of the NLC's machines and the policies*** *which are currently in place, which* ***we will be reviewing*** *as part of the* ***General Controls Review.*** *In the interim, the BoardEffects can continue.*

19.27 Mr. Donald Maphanga, Internal Audit Specialist, sent Advocate Mpumi Nene, CS, an Internal Audit Memo: Security Alert on BoardEffect, via email, on 28 September 2020. He informed her that: (**Exhibit H3.9**)

BoardEffect was always allowed to pass the security scanning (whitelisted), the only issue started when Mimecast discovered that js file.

The reason that link was deemed harmful site, Mimecast blocked that URL because it has. JSfile in it. Mimecast always update their URL Protection Definitions configurations threats that are discovered on a regular basis, tomorrow it might be something different as cybersecurity threats and controls keeps changing on a regular basis.

19.28 As per the Internal Audit Memo: Security Alert on BoardEffect, the following: (**Exhibit H3.9**)

1. Background

On the 05 May 2020, CFO (CFO) attempted to access BoardEffect through a link from BoardEffect, Mimecast which is NLC's email security partner flag the link as possible harmful site. The CFO immediately notified the CIO (CIO) about the incident, thereafter contacts were made with Vox Telecom (appointed service provider for the NLC email hosting partner) to establish and understand the security alert. BoardEffect was also contacted to report the incident through the office of the CS.

1. Recommendations

Based on the information reviewed, the security incident did not result in exploitation (hacking) of the identified vulnerability and the .js file was flagged and blocked based on Mimecast URL Protection Definitions configurations/settings. Through observation and walkthrough on BoardEffect with the CIO, the link that was considered harmful on 07 May 2020 by Mimecast was used again to

try and see if it will be labelled as harmful site, it noted that the CIO was able to log into BoardEffect using the same link flagged Mimecast, previously.

...BoardEffect should consider performing a penetration test or external vulnerability assessment to assess whether that vulnerability identified by Mimecast can be exploited by a hacker and possibly share the results with NLC.

...BoardEffect must provide a guarantee that the java script used is not harmful and BoardEffect must further advise the NLC on whether the link should be whitelisted to avoid further alerts.

19.29 Ms. Farhana Suder, Group Head Legal Governance, Human Resources from BoardEffect sent the Commissioner, Ms Thabang Mampane the following reports on 12 October 2020, via email: **(Exhibit H3.10)**

1. *General Cybersecurity Controls Review Report (presented to management, received comments and finalised Report incorporating management's comments)*
2. *External Penetration Testing and Web Application Assessment Report (presented to management today, circulated to management for comment)*

19.30 On 13 October 2020, Attorney, Farhana Suder sent the Commissioner, Ms Thabang Mampane, via email, an Internal Vulnerability Assessment and Penetrating Testing Report and an Excel Spreadsheet containing all the identified vulnerabilities. **(Exhibit H3.10)**

19.31 NEO Solutions submitted the following documentation, signed on **26 October 2020,** after performing the work: **(Exhibit H3.11)**

i) SBD4 – Declaration of interest;

ii) SBD8 – Declaration of Bidder's Past Supply Chain Management Practices; and

iii) SBD9 – Certificate of Independent Bid Determination.

19.32 "Penelope" pulled a CSD Registration Report on **27 October 2020**. As per the CSD report, NEO Solutions is a level 1 B-BBEE contributor. **(Exhibit H3.12)**

19.33 NLC issued Requisition 18674 for an IT assessment and advisory. Mr. Skhumbuzo Mahlambi, Executive PA Commissioner was the requester, and the **need-by-date** was **02 November 2020**. The requisition was for **R498 000.00**. **(Exhibit H3.14)**

19.34 The NLC issued **purchase order** 10642, dated **27 October 2020**, for an IT assessment and advisory, for **R498 000.00**, thus after services commenced. **(Exhibit H3.13)**

19.35 NEO Solutions submitted an **invoice**, invoice number NEO10490, dated **28 September 2020**, for IT assessment and advisory (as per the attached interim status report) for R498 000.00. **(Exhibit H3.15)**

19.36 The following anomalies were identified pertaining to the invoice submitted by NEO Solutions **(Exhibit H3.15)**

i) There is no logo or branding on the invoice; and

ii) An FNB bank account opened in Centurion reflects on the invoice and not the Standard Bank, bank account as per the previous invoice.

19.37 The NLC made the following payments to NEO Solutions during the period May 2017 to September 2020: (**Exhibit H4.1**)

Date of Invoice	Invoice Number	Description	Amount (incl. VAT)
23 May 2017	NEO10985	Services rendered for the removal, delivery, verification and reconciling of 3rd Lotteries Licence bid documents from SARB to NLC Offices	R145 190,40
31 July 2017	NEO10990	Interim fee for the period 21 June 2017 to 31 July 2017 for services rendered: Factual findings on Ithuba's compliance with the Licence Agreement and related issues	R1 286 388,54
19 September 2017	NEO10995	Final fee for services rendered for Phase 1 of 4: Review of the business plan of Ithuba for the 2018 financial year	R343 412,46
23 February 2018	NEO10960	Interim fees Interim Fees for services rendered for forensic and risk requirements by NLC and for attendance at disciplinary hearings, as approved Interim Fees for attendance to issues relating to Court action instituted by the former Licence	R442 667,93
30 March 2018	NEO11046	Interim fee for professional services rendered for Phase 2: Development of Knowledge Management Hub (05 February 2019 to 30 March 2018)	R2 500 000,00
21 May 2018	NEO11048	2nd Interim fee for professional services rendered for Phase 2: Development of Knowledge Management Hub (05 February 2019 to 30 March 2018)	R486 386,00
28 September 2020	NEO10490	IT Assessment and Advisory – as per the interim report	R498 000,00
		TOTAL	**R5 702 045,33**

19.38 An interview was conducted with Mr Mothibi Ramusi, CIO, on 13 December 2022. As per the interview: (**Exhibit N5**)

i) the culture in the organisation is that when the users receive a suspicious email, a call will be logged;

ii) there was an incident where the former CFO, Ms Xolile Ntuli received a suspicious email;

iii) there was a board meeting, to protect the meeting, he notified the CS or the Commissioner that the CFO, received a suspicious email

pertaining to BoardEffect and advised to stop recording for security purposes in order for them to investigate the incident;

iv) the following transpired:

- Step 1: CIO received a call from the CFO pertaining to the suspicious email;
- Step 2 & 3: CIO alerted the Chairperson of the HCM Board Committee and the CS;
- Step 4: ICT logged a call with VOX to conduct a trace;
- Step 5: CIO alerted the BoardEffect team about the alert message;
- Step 6: CIO shared screen shots with BoardEffect for records;
- Step 7: BoardEffect acknowledged receipt of NLC query;
- Step 8: Mimecast advised on how to deal with the suspicious link;
- Step 9: CS requested CIO to share an incident report to Commissioner;
- Step 10: CIO submitted an email report to the Commissioner;
- Step 11: Commissioner addressed the letter to BoardEffect;
- Step 12: VOX Telecom responded;
- Step 13: Mimecast provided explanation pertaining to the Java script;
- Step 14: Mimecast findings;
- Recommendations to the Board.

v) he was requested by the Board to draft an incident report, the report was provided to Ms Anashnee Maharaj, until then the Board discontinued the use of BoardEffect, until receiving clearance;

vi) after a day or two he realised that the email was not harmful, however what they did for prevention was not wrong;

vii) he only became aware of the appointment of NEO Solutions after the incident;

viii) he was then asked whether he was certain that people were not able to login remotely. He indicated that he had not come across any instructions that warrants big issues;

ix) the Commissioner asked him to provide them with findings. He submitted a report on 07 May 2020;

x) the former Commissioner called him and informed him that NEO Solutions has been appointed pertaining to the information leakage;

xi) he requested the scope of work from one of the officials from NEO Solutions, it is only then when he realised that they were going to look into BoardEffect, cookies, a product called Mydisclosure for declarations and Policy Manager for their policies;

xii) NEO Solutions was appointed by the office of the Commissioner;

xiii) NEO Solutions was appointed as a consulting company during the third National Lotteries Licensee Operator process, doing adjudication around cyber security; and

the owner of the BoardEffect indicated that based on their investigation the organisation should not be concerned

1.30.