ADDRESS BY MR. J BLOCK (MPL) MEC FOR FINANCE, ECONOMIC DEVELOPMENT AND TOURISM AT LAUNCH OF BIOMETRIC ACCESS CONTROL SYSTEM (BACS) PROJECT ON THE 15TH OF OCTOBER 2013 AT THE MITTAH SEPEREPERE CONVENTION CENTRE.

Programme Director

The Premier of our beautiful Province

Speaker and Deputy Speaker of the Provincial Legislature

Members of Executive Council present here today

Members of Portfolio Committee on Finance, Economic Development and Tourism

Members of Select Committee on Finance of the NCOP present

Representatives of Chapter 9 institutions

The Director General

Heads of Departments

Chief Financial Officers and Departmental Senior Management

System Controllers

Ladies and gentlemen

It is indeed a great pleasure for me to stand before you today on this important day of the launch of the implementation of the biometric access control system. Our core responsibility as the Northern Cape Provincial Treasury is to perform an oversight role to all provincial government departments, municipalities and public entities.

During the tabling of the budget vote speech for Provincial Treasury at the beginning of this year, I indicated that in an attempt to further improve security on government's financial and human resources systems, a Biometric Access Control System is going to be implemented in the provincial administration in the current financial year. I also indicated that the tender processes have been concluded and the final award of the tender to the successful bidder was to be made on the day of the budget vote speech.

We can today safely announce that the successful bidder was Datacentrix and its business partners, i.e. Lawtrust and Indenani who have been commissioned to supply, implement and support the Biometrics Access Control Systems for the NCPT to address the business and technical requirements of the Northern Cape Provincial Treasury.

On the same day I further indicated that the implementation of biometric access control will enhance the integrity of provincial government information technology system from improper access both internally and externally and thereby reduce if not eliminate fraud and corruption perpetrated using government systems. This is the day, it has come, and it is with us today. We are no longer saying it will come but we are saying that day that we spoke about has arrived and is here with us.

Ladies and gentlemen, electronic fraud has become a harsh reality in today's digital society and as Northern Cape Provincial Treasury we have prioritized the implementation of advanced security controls to guard our financial resources against electronic fraud.

One of the challenges that face all organisations whether in public or private sector is that all are prone to fraud and corruption especially in their procurement cycles and payroll. Fraud and corruption in the procurement manifest itself in illicit rebates, kickbacks, dubious supply relationships, etc. etc. while in payroll it relates to mainly fictitious employees (ghosts) and the manipulation of travelling expenses by inflating the rates charged and kilometres travelled.

Whilst the risks can never be fully eliminated, organizations need to implement or have controls in place to reduce the likelihood of this occurring. Instances of fraud and corruption in the procurement cycle are not easy to detect, prove or prosecute. Evidence to this effect can be found in the number of fraud cases that have been brought before the courts and the government losing the cases as it could not prove beyond reasonable double that the accused actually committed the deed.

Whilst the risk of fraud cannot be eliminated entirely, it can be greatly reduced by putting in place measures such as the biometric access control system to deter it from happening. Most procurement and accounting systems including personnel systems are automated; however these systems and processes are driven by people. Hence, it becomes imperative that the quality of those entrusted with these processes is beyond reproach, that they have the required experience, that they are professionals in their fields and to be constantly trained in order to re-skill them.

The implementation of the biometric access control system will ensure the segregation of duties which is a paramount requirement to be implemented in order to minimise the amount of control each individual has over each business process, so that no single individual is empowered to oversee the whole transaction. Hiring the right staff and providing suitable training is therefore imperative if processes are to work correctly. Hence those who will be operating the system will be provided with training on the operation of the biometrics access control system for the system to be effective to deter fraud and corruption.

Fraud in the procurement process commonly occurs when controls are deliberately overridden, by either the individual who knows he will not be challenged, or a collusive group able to use its knowledge to hide fraudulent activity.

In order to mitigate the risk of fraud, existing internal controls, thresholds and procedures needs to be reviewed as frequently as possible, understanding risk management by identifying the risks within the control environment areas susceptible to fraud can be highlighted and corrected. This is needed because even the most carefully designed and tightly controlled system can be circumvented which is a tendency that is growing where individuals collude to defraud government and therefore deny the citizens the level of service delivery expected of government. The implementation of the biometric access control system will help the provincial government to deal with collusive behaviour and bring it to a stop.

Ladies and gentlemen, when and where fraudulent activity would take place cannot be predicted. It can raise its ugly head at the most inconvenient times. Those responsible for managing the organization should ‘expect the unexpected’ and have a fraud response plan in place to deal with this eventuality. The implementation of the biometric access control system will enhance the credibility of the fraud and corruption response plans develop by the provincial departments.

Within provincial government sphere, there is a comprehensive legislative framework governing supply chain management, but is not necessarily sufficient on its own to deal with the current corruption in supply chain management. The two biggest risks areas identified that allow corruption to continue are:

1. Unfettered access to and incorrect use of Basic Accounting System, Logistical Information System and Personnel Salary System.

2. A lack of sufficient prescripts on the processes that must be followed – this allows for a lack of predictability and transparency in the processes that must be followed during procurement and therefore a lack of prescripts makes it difficult, and in some cases impossible, to audit the processes followed in supply chain management.

Programme Director, we are confident that the implementation of the biometric access control system will go a long way to address these deficiencies that the government has identified as the biggest risks.

Recent fraud cases show an increase in collusion by departmental employees and the increase relates to the capturing, approving and authorization of fraudulent transactions on both the Basic Accounting System (BAS), Personnel Salary System (PERSAL) as well as the Logistic Information System (LOGIS). Departments affected by fraud and corruption instituted criminal cases against affected employees but lost cases due to inability to prove beyond reasonable doubt which is requirement in a criminal case. The solution to the problem lies in the implementation of biometrics access control.

Programme Director, biometric-identification technologies collect and analyze unique human traits. A sample is collected from a user, processed into a digital template and stored for later comparisons. Biometrics can be used to verify the identity of an individual or to determine if a record of the person exists in a larger database. In the not-so-distant future, we may access our homes and cars, perform retail transactions, or renew driver’s licenses using our physical traits.

Passwords which are currently being used in the Provincial Government are potentially the weakest link in our information security systems. Biometric authentication technologies promise a more secure alternative. The main benefit of using a biometric authentication factor instead of a physical token is that biometrics can't easily be lost, stolen, hacked, duplicated, or shared. They are also resistant to social engineering attacks – and since users are required to be present to use a biometric factor, it can also prevent unethical employees from repudiating responsibility for their actions by claiming an imposter had logged on using their authentication credentials when they were not present which has been one of the defence mechanisms used by those brought to justice.

Biometric systems can be much more convenient than tokens and other systems, and are useful to augment existing security methods like passwords.

The main drawback of any biometric system is that it can never be 100 percent accurate. To use a biometric system, it is first necessary for each user to sign up by providing one or more samples of the biometric in question such as a fingerprint which is used to make a "template" of that biometric. When a user attempts to authenticate, the biometric they provide is then compared with their stored template. The system then assesses whether the sample is similar enough to the template to be judged to be a match.

Programme director, allow me to remind your audience and listeners at home that it is our priority as the current ruling party to act against any corruption or fraud activities—let me repeat by saying as the current administration we are in efforts to root out fraud and corruption in the public service in order to enhance service delivery to the people of this Province.

Today we live in a democratic, non-racial country and this is a reminder that we always remember that this freedom did not come cheap. Most of our people sacrificed their lives for us to enjoy this democratic right in our mother land. Our government is transparent and that is why you are informed of the happenings in government because it is the government of your choice, it is the government that cares for its people. The biometric access control system implementation will help us protect the financial resources that the public has entrusted with us.

These systems are used to process orders, maintain assets, and pay suppliers and salaries of government employees. We need to be proactive not reactive in order to deliver on our promises as government. These key systems have been identified to have inherent challenges with respect to security controls that could be exploited to create security vulnerabilities that would have a negative financial impact for the province.

Inappropriate and unauthorised access to these information systems could result in inaccurate financial and performance related information being provided to management. Furthermore, is that a key feature by the system is a context sensitive audit trail that provides legally admissible and indisputable evidence to ensure that

offenders can be identified, prosecuted and convicted where applicable. Officials can easily potentially deny that they have committed a transaction because they know that they use it as a legitimate excuse and get away with it.

The NCPT as an organisation exists and participates in both the physical and digital worlds. Most institutions find it significantly challenging to secure and protect their electronic information and digital assets than those in the physical world. In this context the public and private sectors are increasingly falling prey to criminal operations aimed at defrauding organisations for monetary and other commercial gain, costing South Africans billions of rands. This initiative will protect the innocent against computer identity theft and sensitive applications against unauthorized access.

It is for this reason why the province is required to implement a mechanism of handling evidence in an impartial and legally complaint manner, in order to hold individuals accountable for their actions when performing specific transactions.

This new-born implementation will kick-start at the end of the current financial year and will maintain accountability of users – it will also identify who did what when, in terms of all sensitive transactions in BAS, PERSAL and LOGIS. The biometric access control system uses smartcard and advanced electronic digital signature system and it will be for 1700 users within all departments of provincial administration. All critical hardware and software systems have to be of high availability architecture to ensure the highest possible availability of the solution—the solution must be able to operate on the government network (SITA) infrastructure with limited bandwidth. Procurement and the installation of a storage and backup systems to store transaction evidence data will be for two years on line and then for a further 20 years for audit purposes at the specified site.

Our mission statement (as NCPT) clearly states that we “promote sound fiscal policy that enables financial sustainability and supports economic development”. The department has a demanding task in an adverse economic climate of ensuring that the R12 billion allocated to the province is managed properly and is effectively utilized to accelerate service delivery. Currently, the Northern Cape Provincial Government rely on the transversal systems (BAS, LOGIS and PERSAL) to carry out service delivery transactions and the computer systems provide access to Provincial

resources and budget; these newly introduced system will advance the security on current transversal systems and will be implemented into phases—the first phase will be comprised of 30 system users to test how the network handles the pressure.

Programme Director, we take into account that our employees are important assets and we see as a priority to also protect our employees and their identities from being manipulated, stolen and abused by fraudsters or syndicates to commit fraudulent transactions. I am sure you will agree with me that we live in a technologically advance environment hence we find it crucial to guard against electronic fraud and to protect our people's identity. We set to protect the innocent employees.

Ladies and gentlemen, I believe that you are aware that our information systems were designed at a time when the access to the system was based on password; and the password is the only mechanism by which an individual can be identified. These passwords have become vulnerable especially with the advent of modern information security challenges including: spyware, hacking, password sharing and social engineering attacks.

Programme director, syndicates manipulate and identify corrupt officials; work closely with corrupt suppliers. The corrupt officials install spy ware to capture password, and innocent officials become victims because their passwords are often stolen to enable syndicates to access systems such as BAS and LOGIS to generate payments, and for PERSAL system they create payment to ghost workers through stolen passwords. Sometimes these syndicates will persuade a registered supplier for their payments to be transferred to his or her bank account or they will change banking details in the system and direct payments to a changed bank account.

It is for such reasons we opt to embark on this project in order to protect our scarce resources and employees as part of our efforts to combat electronic fraud and corruption. This project will be championed by 1700 BAS, PERSAL and LOGIS users from provincial government departments in the province. We do not want to believe in allegations to create a negative perception or publicity about a person but through this system enough evidence and proof will be produced and culprits will face the music.

We urge public servants, community structures and business people to proactively take actions to minimize the impact of fraud and corrupt activities. Events such as this one provide a platform to utilize opportunities and understand processes which are in different spheres of government—to combat fraudulent activities.
I appeal to all people of this province to come together and build this province for the future of our children—to public servants let us take actions and fight fraud and corrupt activities.

Lastly Programme Director, I would like to acknowledge the presence of the members of executive board of Datacentrix, Mr Kenny Nkosi and Ms Dudu Nyamane as well as Mr Rex Madida the chairperson of Idenani Consulting as well as Mr Maeson Maherry who is the director of Lawtrust Information Security Solutions in our new partnership in the implementation of the biometric access control system

“Working together as public servants we can do more”.

I thank you.