Association of
Former International
Civil Servants of
the United Nations (Kenya)

Briefing Note on Security and Related Investigations*

Policy Brief June 2018

KEY MESSAGES

- People play many critical roles in securing the assets of the State.
- Both National and Local Governments should institute routine, pre-employment screening as part of their sound personnel management procedures.
- Government and employers should ensure that no public servants or professionals remain in one position for so long that they acquire a level of control that may become a security risk.
- Regular security audits are of vital importance to ensure the good governance, transparency and accountability of the President's Four Pillars Agenda.
- Every Government entity should ensure that regular backup copies of important information are made and stored offsite.
- Given the scale of government assets, there is an urgent need to develop a security programme capable of protecting those assets from theft, fraud and corruption.

1. Introduction

This briefing note provides an overview of key security concerns and related investigations; and their role in promoting good governance, transparency and accountability in the President's Four Pillar Agenda for: low cost housing; food security; universal affordable health coverage; and manufacturing.

Role of Security

A wide range of resources are needed to implement the Four Pillar Agenda, including: infrastructure; vehicles and machinery; computers and information; and personnel; all of which need to be safeguarded against misuse. Given that the Government will be disbursing billions of shillings to procure these assets, it is essential that a comprehensive security programme be established to protect them from theft, fraud and corruption.

Challenges

Implementation of the Agenda faces several challenges related to Kenya's security and investigative capacity.

- Most crimes in Kenya are not reported because of a general lack of confidence in the police and the country's judicial system. Many reported crimes are not investigated, which has led to public apathy about reporting crimes. Furthermore, many criminal cases when taken to court are thrown out on the grounds of poor investigation and un-coordinated evidence. Other cases, such as fraud and cybercrime, are complex and the police lack the necessary investigative capacity, expertise and forensic facilities for the thorough analysis of evidence.

- Many cases are currently pending to be heard, some dating back more than ten years. This is due to a shortage of magistrates and judges; and those that have been appointed are overwhelmed by the large number of cases allotted to them. Delays are also attributed to lack of integrity and corruption, where some criminal justice officials, notably among the police, as well as among prosecutors and magistrates/judges, conspire to subvert the wheels of justice. Regrettably, for several consecutive years, Transparency International has ranked the National Police Service as the most corrupt institution in the country. Recently, local media has reported that original files relating to the Anglo Leasing case cannot be traced at the Attorney-General's office, a case that has remained pending before the court for more than a decade.

- Lack of infrastructure for rapid and effective response undermines police capacity to deal with crimes and conduct investigations. Police

*I wish to acknowledge and thank Mr. Jesse Ngari, AFICS-Kenya's security expert, for his major contribution to this brief. Please note, however, that the views and opinions expressed do not necessarily reflect those of AFICS-Kenya.

Amb. John O. Kakonge,
President, AFICS-Kenya

AFICS-Kenya
c/o United Nations Office at Nairobi, Gigiri,
Central Area, Main Lobby;
P. O. Box 47074-00100, Nairobi, Kenya
Email: afics.kenya@un.org
Phone: +254 20 76 23531
www.afics-kenya.org/consultancy
www.afics-kenya.org

lack transport and equipment; and most importantly, the National Police Service's capacity to conduct forensic investigations is limited. This has been partially addressed after the police leased 2,000 vehicles from Toyota Kenya. Recently, the President requested the Communications Authority of Kenya to give the police KSh.1 billion to set up a forensic laboratory at the Headquarters of the Criminal Investigation Department, Kiambu Road, Nairobi.

- Many victims and witnesses tend to shy away from giving evidence in criminal proceedings due to the absence of effective protection mechanisms. Some progress has been made, however, with the enactment of the Witness Protection Act (Government of Kenya, 2006), which provides a legal framework and procedures for the protection of witnesses and the establishment of a victim protection agency. According to Section 3B(1) of the Act, the objective of the agency is to provide "special protection, on behalf of the State, to persons in possession of important information and who are facing potential risk or intimidation due to their co-operation with prosecution and other law enforcement agencies". The effectiveness of the Agency, however, has been mixed because it has not been adequately resourced to manage the complexities of witness protection.

- Coordination between partners in Kenya's judicial system: the police, the prosecution and the judiciary, is weak. Each agency tends to work independently, or within its own legal mandate; and the nature of the partnership remains undefined, with no legal backing. Furthermore, there is no common database for sharing information between agencies, which enables previous offenders to go undetected as they are processed through the criminal justice system.

2. Components of a Good Security Plan

A physical security plan or programme should include policies and procedures, which define the security controls that need to be put in place. For example, deterrent controls, such as perimeter fences and security guards are used to prevent or discourage any attempted breach or intrusion. Delaying controls – locks and access controls – are aimed at slowing down the intruder in achieving their objective. Detection controls, such as closed-circuit television (CCTV) and smoke and fire alarms, are useful for early detection of incidents. The plan should also have a specific component detailing how it will be audited, including the maintenance of access records (registers) to key facilities; and a requirement that all visitors and employees provide an identification document (ID) or staff badge before entering restricted areas.

3. Personnel Security

During implementation of the Four Pillars Agenda, human resources will play a central role in securing the assets of the National and Local Governments. Hence, it is critical that the Government develops security policies and procedures aimed at ensuring that their personnel do not become a threat to the security of assets. These measures would help the Government to employ reliable people; minimize the chances of public servants becoming unreliable, once they have been employed; detect suspicious behavior; and resolve security concerns once they emerge.

Potentially Harmful Employee Activities

Some of the potentially questionable or suspicious activities in which public servants may engage include: fraud and theft, which may be committed alone, or in collusion with third parties for personal gain; and bribery and corruption, entailing misuse of official authority for personal profit, or cause financial loss to the Government.

Unintentional disclosure is another potentially harmful activity that occurs when public servants are unaware that they are disclosing valuable or sensitive information. Examples include: leaving an office unlocked; not securing a password; or allowing the theft or loss of security passes, laptops and mobile devices. Unauthorized disclosure of information may also take place when a public servant deliberately releases sensitive information, driven by malice or financial gain.

Other possible illegal activities include cybercrime, which involves using computers and other forms of information technology (Osterburg and Ward, 2014). An example is hacking, where a computer network is broken into and personal or confidential information is accessed to facilitate fraud. Another is identity theft, where an offender illegally uses another person's identity without his or her knowledge or consent to commit fraud or other crimes. According to paragraph 3.1 of the Prudential Guidelines of the Central Bank of Kenya (2013), money laundering is defined as a process by which criminals attempt to conceal the illegal origin and illegitimate ownership of property and assets that are the fruits or proceeds of their criminal activities. Similarly, procurement fraud targeting students of state schools, could occur if the annual KSh.4 billion National Hospital Insurance Fund (NHIF) is misused by medical facilities by unnecessarily admitting students to obtain higher NHIF disbursements. Other cases may involve inflated or forged claims submitted to NHIF. Mortgage fraud may also be committed when tendering for or implementing the construction of the 500,000 low-cost houses under the Four Pillars Agenda.

4. Proposed Preventive Measures

Pre-employment screening is the foundation of good personnel security, including: vetting; due diligence; and background checks. Besides annual staff appraisal, continuous evaluation of employees who hold sensitive positions, or where there is some evidence of suspect behaviour should be conducted. Background checks include: criminal history (CID certificate of good conduct); credit status from credit reference bureaux; and lifestyle audit.

One of the best practices for mitigating risks to assets from employees who are most likely to do harm (Raytheon, 2009), is the careful management of employees: whose employment has been terminated; have resigned; or are about to resign. Measures include: requiring such employees to leave the facility immediately; surrendering any work ID; and returning any Government property in their possession. Likewise, privileged access credentials, such as passwords should be changed, or disabled immediately. A recent, ongoing court case relates to an incident where passwords of retired/former Kenya Airports Authority employees were used to clear 124 containers without paying over KSh.100 million customs duty or tax.

Further, separation of duties is important to make sure that one individual cannot complete a critical task on their own to reduce the potential for theft, fraud, information leaks and other breaches of security. Rotation of duties and assignments is an effective administrative and detection control that can be put in place to uncover fraudulent activities or misuse of resources. No public servant should stay in one position for extended period, because they may acquire too much control over a specific segment of operations. All employees, particularly those in sensitive positions, should be encouraged to take their annual leave. Once they take leave, other individuals can step in and may be able to detect any fraudulent errors or activities.

Whether manual or automated, access controls are important in controlling entry to physical or electronic assets by unauthorized individuals. Access control measures include: physical barriers; locks; security guards; and bollards. Protective monitoring involves installation of monitoring devices, such as closed-circuit television (CCTV) and intrusion detection expert systems (IDES), especially in sensitive areas, to provide real-time alerts on unauthorized access.

Public servants who commit fraud and theft should be exposed and legally pursued, not least to discourage and deter others from committing similar unlawful actions. Prompt investigation, successful prosecution and recovery of stolen assets/funds are major deterrent strategies to fighting fraud and theft in both national and local levels. For instance, in March 2008, the local media reported that two senior civil servants in the Ministry of Local Government were convicted of irregular practices in the purchase of a 120-acre parcel of land for a public cemetery in Athi River, Machakos. The offence of corruption was proved, and each accused person was sentenced to two years' imprisonment and fined KSh.40 million and KSh.37.2 million, respectively.

With regard to cybercrime, computer systems should be kept up-to-date and personnel be provided with/or create strong passwords to access information to deter hackers. Personnel should also be encouraged to change passwords frequently. To prevent money laundering, banks should know their customers, so that before opening an account for a new customer they should establish strict due diligence rules, such as authenticating or verifying a customer's identity through production of ID, or passport. The Prudential Guidelines of the Central Bank of Kenya (CBK, 2013) stipulate that "the need for institutions to know their customers is vital for the prevention of money laundering and underpins all other activities." Another preventive measure is that banks are required by CBK to ensure that cash transactions of over US$10,000 require a customer to complete a form declaring source of funds, purpose and identity of the beneficiary.

Security awareness training should also be conducted to sensitize public servants to understand the importance of securing National and Local Governments assets in realizing the goals and objectives of the Four Pillars Agenda and other programmes. Such training must be supported by senior public servants, and National and Local Governments must allocate adequate resources for this activity and enforce attendance.

Information Security

Information and communications technology (ICT) is crucial to both National and Local Governments in the attainment of the Four Pillars Agenda. New and emerging security risks, however, expose ICT resources to multiple security threats. Hence, there is a need to formulate security measures aimed at ensuring: availability of information to authorized users only; confidentiality; safeguarding information from unauthorized access; and ensuring integrity that entails protection from intentional, unauthorized, or accidental changes of data.

Threats to Information Technology Assets

In an ICT system, data exists in three states: 1. Data at rest, which are stored in servers, databases, and on internet sites, laptops and mobile devices, for example; 2. Data in motion, or in transit, flowing across internal networks and to the outside world; 3. Data in use, being accessed or used by the system at a point in time, such as an open document, a file being copied to a USB drive and data being copied and pasted from one document to another.

Regardless of the state of data, they are subject to numerous threats, such as unauthorized disclosure of information by personnel either intentionally or unintentionally. Other threats may materialize by: using weak passwords; transmission of passwords over the network without encryption; and carelessness of users leading to attacks by viruses that can damage or corrupt a system. To mitigate these, regularly backup of important information and offsite storage are essential.

Controlling Access to IT Assets

Controls fall into three major categories: 1. Administrative controls, which include security policies and procedures. Policies spell out the dos and don'ts of using ICT assets, such as: computers access rights; separation of duties; security awareness; security review; and audit reporting to determine whether users are adhering to policies and procedures. 2. Physical controls are concerned with constraining direct physical access to ICT resources by unauthorized persons, including: door locks; key cards; security guards; and alarms. 3. Technical controls are implemented through hardware or software that is typically difficult to defeat once in place and can work without human intervention. These include: anti-virus software and antispyware; encryption; audit trails; and intrusion detection expert systems designed to detect unauthorized use, hacking or any suspicious activity.

All these measures must be documented in an information security policy to protect sensitive information. The policy is aimed at educating users on handling and protecting confidential and sensitive data, and the consequences of violation. The policy must be communicated to all employees through information security training, which is important because the security of ICT assets in National and Local Governments depends upon technology and people; and people are usually the weakest link and cause most security breaches and compromises.

Proactive Criminal Investigation?

The purpose of criminal investigation is to gather admissible evidence that may lead to placing the offender/s before the courts (New Zealand Government, 2015). Criminal investigation involves the collection of information and evidence for identifying, apprehending and convicting suspected offenders (Osterburg and Ward (2014), and is based on three major sources of information – people, physical evidence and records, including social media, such as Facebook, Twitter and WhatsApp.

Proactive criminal investigation is a preventive or anticipative approach of inquiry into potential crimes occurring, and associated risks should they occur. It is geared towards deterring the occurrence of criminal acts and reduces the harm they are likely to cause.

5. Conclusions

- Cost-effective, security policies, systems and procedures for the protection of assets are required at both National and Local levels to ensure their efficient and effective use, and realization of the President's Four Pillars Agenda.

- Government must develop procedures to protect its personnel; at the same time, it is essential to adopt measures that ensure that positions of trust within the civil service are not abused. Such procedures and measures will protect the assets whose security is under threat..

- Information communication and technology assets must also be protected from unauthorized disclosure and emerging security risks.

- Potential breaches of security relating to assets procured for implementation of the Four Pillars Agenda require both proactive and reactive investigations to demonstrate good governance, transparency and accountability.

- Working closely with other key stakeholders, AFICS-Kenya offers a range of security advice and investigatory services through its extensive network of consultants, with the necessary national and international expertise, experience and exposure to provide independent and objective advice and support.

References

Central Bank of Kenya (2013). "Prudential Guidelines for Institutions Licensed under the Banking Act." pp. 203–207, 220–221.

New Zealand Government (2018). "Reporting incidents and coordinating security investigations." Section 4.2. *https://protectivesecurity.govt.nz/governance/reporting-incidents-and-conducting-security-investigations/*

Osterburg, J. W. and Ward, R. H. (2014). *Criminal Investigation:* A method of reconstructing the past. Seventh Edition, Elsevier Inc, 5, 265.

Raytheon Oakley Systems (2009). "Best practices for mitigating and investigating insider threats – Whitepaper." *https://www.raytheon.com/capabilities/rtnwcm/groups/iis/documents/content/rtn_iis_whitepaper-investigati.pdf, 1–6.*

Republic of Kenya (2009). "Proceeds of Crime and Anti-Money Laundering Act", No. 9 of 2009. Laws of Kenya, pp. 13–14, 29–32.

Republic of Kenya (2006). "Witness Protection Act", Chapter 79, Laws of Kenya. pp. 6–7.