IM25: THEMATIC ASSESSMENT

SECURITY VULNERABILITIES IN GOVERNMENT

October 2009

1. INTRODUCTION

1.1 *Persistent concerns around information security risks in the government are assessed as a **major risk of long-term duration**.*

1.2 Foreign governments and their intelligence services strive to weaken the State and undermine South Africa's sovereignty. Continuing lack of an acceptable standard of security at client institutions (government departments, parastatals and national key points) increases the risk. With the formation of the new government and its electoral mandate carried out in key priorities and programmes, particular ministries and their respective departments are becoming targets of foreign intelligence services (FIS) for opportunities and influence.

1.3 Previous and current investigations by NIA indicate that the human factor remains the primary cause of security vulnerabilities at client institutions. This resulted in an array of security-related incidents, such as security breaches, the theft of personal and laptop computers and other information and communication technology-related equipment at client institutions over the past few months. The aforementioned demonstrates the extent of non-compliance with information security policies and non-implementation of the Minimum Information Security Standards (MISS), which continue to represent a major risk to the integrity of sensitive/classified information.

1.4 Similarly, investigations concluded by the National Intelligence Agency (NIA) have exposed serious deficiencies in the security integrity of the information and communication technological systems (ICTS) at a number of client institutions. Investigations revealed the extent to which these weaknesses were exploited for fraudulent purposes and financial gain. Whilst fraud and concurrent financial losses to the government raises concern, deficiencies exposed by these incidents have far-reaching strategic implications. Such deficiencies render statutory institutions vulnerable to fraud and corruption, and worst to espionage and malicious infrastructural disruption.

2. TRENDS ASSOCIATED WITH SECURITY DEFICIENCIES IN GOVERNMENT

2.1 Security deficiencies at client institutions remain a standing challenge. Personnel, physical, document and information communication technology security remain prevalent deficiencies.

2.2 NIA has established the following trends that underline security vulnerabilities

- Non-adherence to the MISS regarding the criteria for classification of documents and control of information (the aforementioned has been reported nationally);
- Non-issuing of security clearances /record checks on external courier services transporting classified documents;
- Insufficient lock-up facilities to store classified information and the lack of control over copies and/or the removal of sensitive information from Client Institutions (the aforementioned has been reported specifically in Mpumalanga, Limpopo, North West and KwaZulu Natal);
- Non existence of control measures and/or procedures for the destruction of sensitive/classified documents.
- Limited vetting of senior officials employed at sensitive institutions. ICT personnel in particular are often not being vetted;
- Inadequate protection of the storage and retrieval of information (sensitive and classified);
- Recommendations made during security audits at Departments are often not being implemented;
- No approved encryption facilities on landlines and/or cellular phones;
- No records with regard to the transmission and receipt of all sensitive information via facsimile and no effective control over open facsimile machines;
- Virtually uncontrolled access to ICT and communication equipment;
- Non-adherence to MISS in terms of using encryption for computerised transmission of sensitive/classified data;
- The lack of proper ICT emergency plans and procedures and disaster recovery plans in terms of information stored on networks;
- A general lack of skilled personnel to implement and maintain effective ICT security;
- No institution responsible for performing formal back-up/ restoring procedures or to test the functionality of ICT systems. Institutions that do have own measures in place are making use of un-vetted contractors with facilities which are non-compliant with minimum security standards;
- Most Client Institutions outsource their ICT functions to private companies of which only a few undergo record checks;

- No password protection of laptop computers. Inadequate control over the issuing of laptop computers and the removal/storage of such computers away from Client Institutions;
- The appointment of Security Managers remains a concern. It should be noted that the Security Managers Forum (SMF) is a sub-committee of the Counter Intelligence Coordinating Forum (CICF), and as such report to the CICF. In many instances the criteria set for filling these positions are not met. In some instances Security Managers have not been appointed as yet. Another challenge that remains is that, in some instances, Security Managers are not appointed at the level of a Director, as stipulated in NIA's position paper on the issue, which result in the lack of adequate communication between Security Managers and their senior management, ultimately negatively impacting on security in that Department;
- Closely linked to the aforementioned is the fact that Security Manager's Forums in some provinces are not functioning (such as in the Northern Cape, The Forum in the Eastern Cape was only reactivated in 2009, after being dormant for two years);
- It has been determined that coordination on provincial level with the SMF remains insufficient;
- A trend has been established that Security Managers do not report incidents of security breaches to NIA as they fear that the incident would negatively reflect on them personally and/or their Department;
- A questionnaire, developed by the Counter Intelligence Coordinating Committee (CICC), to report security breaches, has not been implemented by the SMF.
- Finally, Security Managers are not being held accountable for the implementation of the MISS in their Departments.

3. THE CURRENT THREAT POSED TO CLIENT INSTITUTIONS ITO SECURITY VULNERABILITIES

3.1 In addition to the aforementioned, the following section provides a somewhat more detailed exposition of vulnerabilities that have been identified at Client Institutions, which could be exploited by foreign and private intelligence services/structures as part of their espionage efforts:

- **Inadequate awareness among government officials of the threat of espionage posed by foreign intelligence services.**

Although certain Government institutions have been reached through the implementation of the MISS, security consciousness remains deficient. In this regard the problem of naivety among employees at sensitive installations, government departments and even private institutions and businesses mainly stems from a lack of knowledge regarding the threat posed to South Africa in

general. The aforementioned results in South African citizens assisting/co-operating with foreign intelligence services, whether by unwittingly providing them with classified information or by allowing them access to restricted areas.

NIA, from a defensive perspective, frequently provided security awareness interventions at government departments. In this regard, specific programmes were presented to the SANDF, SAPS, NCC, COMSEC, SASS and others. The security awareness programme included an awareness of the espionage threat as well as focussed on security deficiencies and the impact it has in terms of security in Client Institutions in general. A similar awareness intervention was presented to provincial clients, such as the Treasury in Limpopo (Polokwane). However, from a provincial perspective, many provinces reported that security awareness in their provinces are either not being conducted or that it is inadequate.

- **Exploitation of protocol privileges for intelligence purposes inter alia, the lack of control of diplomats placed in South Africa and non adherence of accreditation protocols by foreign diplomatic missions in the country. In addition, foreign intelligence service members utilise diplomatic cover to obtain access to sensitive information through their contact with government officials.**

  The activities of some FIS members are characterised by a total disregard for the regulations and protocols governing the conduct of diplomats and their staff. Diplomatic cover is also frequently being used to obtain access to certain individuals and institutions, particularly Departments such as the Department of International Relations and Cooperation (DICO). FIS members also use their diplomatic status to gain access to critical information and/or infrastructure, where they can freely establish contacts in various sectors of the South African government and economy. An example of the former is the free access to the Oliver Tambo International Airport (ORTIA) by the Security Manager of the Israeli airliner, EL AL.

  Interestingly, vetting statistics confirmed the fact that DICO remains specifically problematic. DICO had the highest number of security clearances being denied, followed by the then Directorate for Special Operations, the Department of Trade and Industry and then the Department of Home Affairs. Security clearances were denied due to the following: dual citizenship, drug/substance abuse, contact with FIS, poor financial management of personal finances and a lack of cooperation to the vetting investigation process.

- **Limited measures and lines of communication exist whereby South African Government Departments could inform NIA on agreements and arrangements with foreign countries. No information on various**

Committees and sub-Committees operating in government is being liaised with NIA.

This holds specific threats to national security since FIS members and/or their countries of origin regularly enter into agreements with South African Government Departments, without the knowledge of NIA, which could negatively impact on government programmes and/or interests. Consideration should be made to involve individuals (government officials) with specific skills to be involved in scrutinising potential agreements between government entities and foreign entities, especially those dealing with complicated and specialised issues such as science and technology.

The fact that many inter-departmental and governmental Committees and sub-Committees are operating without NIA having knowledge of and/or advising on possible inherent risks in this regard is currently being addressed by the Counter Intelligence Coordinating Committee (CICF). This situation is regarded as being pivotal since the functioning of many of these Committees directly impacts on national security. Committees that would be scrutinised include those dealing with weapons control and export procedures as well as those dealing with the coordination of terrorism issues.

- **Inadequate control and regulation over the activities of FIS members and/or liaison officers placed in South Africa.**

FIS members regularly liaise with different components of the SA intelligence community. The aforementioned is to a large extent not co-ordinated within the South African intelligence community, which could be exploited by foreign services.

Another factor which poses a threat to South African national security, is the lack of control of access to the offices of government employees and those employed at strategic institutions in the country. In this regard, it is evident that FIS members continue to enjoy uncontrolled access to the Departments of International Relations and cooperation (DICO) and Trade and Industry in particular, especially when utilising their diplomatic cover as indicated earlier. Foreign embassy staff almost have total freedom of access to especially DICO. FIS members also have access to parliament as well as the offices of provincial governments. FIS operatives not only have access to government departments, but are frequently visiting security installations. Visiting delegations (including delegations from Iran and China) to strategic installations such as DENEL, KOEBERG and Mossgas utilise official access, usually on invitation of these institutions, to demand access to sensitive plants where advanced technology is being developed.

The access of FIS is not restricted to officials of Departments such as DICO, but also includes their interest in obtaining access to specific Ministers. In this regard some FIS showed an interest in the Ministers of Energy, Defence and Military Veterans, Minister in the Presidency on Performance Management and Evaluation, DICO and also focused on the office of the President in particular.

Diplomats and FIS are not the only ones exploiting the inadequate security (lack of control of access in particular) at government offices and installations. Private security companies are of specific concern in this regard.

- ***Prospective job applicants in the public sector are not properly screened and foreigners are appointed in sensitive positions without the required security clearances. In addition, current personnel are not frequently enough being re-vetted.***

The non adherence of pre-employment screening, screening of companies and screening of immigrants remains a challenge in client institutions. On the other hand, infrequent vetting of personnel continues to be a noticeable trend.

In terms of conducting Personnel Suitability Checks (PSC), the former had been identified by Cabinet in order to screen individuals prior to employment, as the vetting process fails to yield timeous information on which the decision should be based in terms of employing individuals. The Minister of Public Service and Administration instructed departments to commence with the PSC as from 1 January 2008.

NIA is to, according to an instruction by Cabinet; improve its vetting capacity to 365 vetting functionaries by 2011. The instruction by Cabinet also prescribed the establishment of Vetting Fieldwork Units (VFU) in specific government departments. Out of the 17 priority Departments, only nine had been established successfully, one is semi-functional, five are in the process of being established and two are not functioning.

It is evident that foreigners (who meanwhile naturalised as South African citizens) employed in South African government departments could also pose a threat to national security. The appointment of technical advisors, under the guise of providing aid, also creates vulnerabilities in government departments. The technical advisors, who are responsible for the practical administering of projects, are placed on a national, provincial and local level across South Africa. The uncontrolled access provided by the formal bilateral aid agreements and placement of technical advisors across South Africa is being exploited for intelligence collection purposes. The possibility exists that some of these technical advisors could be employed in potentially sensitive positions in national departments and provincial legislatures where they might

have access to classified information. No regulatory measures are in place to regulate or monitor such activities.

The appointment of foreigners at sensitive installations (National Key Points) remains problematic. Examples include the employment of individuals with scarce skills such as scientists, which are employed in laboratories and research facilities, thereby having access to classified information and/or the process of developing specialised technology. The risk in terms of skills transfer and technology-transfer is enhanced by this practise. Adding to the concern is the fact that the majority of these individuals are employed on a contract basis, which could have an affect in terms of their loyalty to the Institution. However, foreigners are not only employed in these fields only, cases have been reported of foreigners being employed at the State Information and Technology Agency (SITA), the Department of Trade and Industry, Treasury, etc.

The involvement of foreigners, mainly as consultants to the 2010 FIFA World Cup Tournament to provincial clients (host cities), is also posing a risk in terms of sharing classified information with such entities. It is known that foreigners, in many instances, form part of Provincial and other government meetings, where they have access to privileged information. It is also believed that the risk could be extended well beyond the closing of the Tournament. The aforementioned is not limited to the 2010 Tournament, but is valid for all major special events being hosted by South Africa.

It is evident that the screening of foreign nationals remains a grey area and that there is little control over the process. During a recent CICF meeting it has been suggested that the uniform vetting standards be reviewed in order to address this issue. The problem seems to be the lack of guidance to institutions in conducting such screening. Subsequently departments are not adhering to the prescribed annual reporting of the security competency of foreigners in their employment.

- ***Private security companies, many of whom have connections with foreign intelligence services, are recruiting former intelligence members.***

  There is a proliferation of private security and intelligence companies who provide services to and thereby have access to sensitive government, parastatals and private institutions. Clients of Private Intelligence Organisations include foreign embassies, government departments, the private sector, parastatals and foreign-based clients. At present these private intelligence organisations and groups sell their services to whoever is willing to buy them. Apart from possible access to sensitive information, those involved in physical security has access to CCTV footage, which could also

be of interest/value to FIS and an array of other actors. The problem with private security companies is that they are not operating under the same accountability procedures as statutory intelligence structures.

Former and serving members of the government security establishment are recruited by private security companies in order to utilise their expertise, skills, and contacts or to make use of their access within the said institutions. It is known that the American Embassy in Pretoria particularly recruits former SAPS members as security officers, who then maintain and utilise their contacts within the SDAPS and other government departments. It is suspected that these companies still utilize their old contacts in the NIA, SASS, SANDF, SAPS and other government structures wittingly/unwittingly to obtain information.

Private Intelligence Organisations thus potentially provide a perfect conduit for foreign intelligence services (FIS) and organisations hostile to the State who are seeking access to sensitive / classified information from South Africa.

- ***Inadequate security to protect tender documentation***

The lack of adequate security measures, and access control in particular, resulted in serious incidents which have the potential to directly impact on national security. In one such instance sensitive documentation relating to a prominent tender process was being tampered with, which could ultimately result in litigation by those involved.

- ***Security breaches of Technical Information Systems***

It was recommended in the previous NIE that the state should improve the management and coordination of its ICT resources as well as protective strategies and systems. It was stated that the lack of uniform policies, ICT systems and common platforms creates vulnerabilities. When assessing the current status of ICT security in government, it remains evident that the situation has not improved significantly since then.

The improper control over and/or use of laptop computers in particular continue to pose a threat to information security. Numerous investigations have been conducted on the theft/lloss of these computers, which in most instances occurred as a result of negligence. In many instances such laptop computers contained official documentation and were not password protected. The majority of these cases proved that it remains to be difficult to prosecute officials found guilty and that at most, such individuals are being charged with internal disciplinary action. The inadequate control over such computers therefore mains a concern.

The outcome of NIA investigations in the past year signalled a disconcerting trend of breaches in the security integrity of ICTS. The following serve as illustration:

- **The former Department of Foreign Affairs (DFA)**. Since 2006 NIA has been involved in investigating, under operation Phantom, a series of incidents at the then DFA, involving a scam (involving unauthorised access to and fraudulent usage of ICT systems) to register ghost workers on the DFA system, whereby the state was defrauded of millions of rand. Since then, numerous similar cases have been reported, including the latest at the Department of Health, which is currently being investigated.

- **Gauteng Shared Services Centre (GSSC).** In June 2009 a security breach occurred at the GSSC with the intention to defraud of GSSC. Fifteen individuals intended to defraud the GSSC. Of these fifteen, five were GSSC employees – two of whom were part of the GSSC Technology Support Services SAP Unit. The plot entailed the unobtrusive, remote accessing of the Basic Accounting System (BAS). This system processes all payments in the Gauteng Province as part of GSSC's core function of providing government internal support to Audit-, Human Resource-, Procurement-, Finance- and Technology Support Services.

- **Department of Public Enterprises (DPE) in April 2009**. In April 2009, a forensic analysis conducted by NIA on a laptop of a DPE official revealed the presence of eight malicious software applications downloaded which constituted a threat not only to optimal functioning of DPE's ICTS and its business processes but also to the Intellectual Property (IP) residing in the department as it related to parastatals, eg ESKOM, Denel, South African Airways and Transnet.

- **Department of Sport and Recreation**. An employee of the DSR attempted to fraudulently transfer R13 million from the DSR to his personal bank account. The system's time-delay default prevented the transmission of the full amount, resulting in only R955 000 successfully transferred.

- **Companies and Intellectual Property Registration Office (CIPRO**). A two-year investigation, jointly by the Receiver of Revenue and the South African Police Service, into the activities of the Companies and Intellectual Property Registration Office (CIPRO) has revealed widespread corruption in CIPRO. The latest incident involves the fraudulent utilisation of CIPRO's website by unidentified syndicates, assisted by CIPRO employees, who set up and/or registering duplicate or counterfeit companies. In some instances, directors of companies are

fraudulently replaced by individuals using stolen identities. The duplicate companies or fake directors are then used to re-route money intended for the legitimate company by informing clients that bank details have been changed and advise them to send payments to the new account.

In this regard 114 duplicate companies, including duplicates of Nampak Tissue, Avusa Media, Adcock Ingram Housecare and BJ Engineering, have been set up using the CIPRO website. The investigation so far revealed that, over the past two years, corrupt officials at CIPRO have facilitated hundreds of scams which have impacted on revenue income of government, a number of prominent companies, and hundreds of smaller private businesses.

It was carried in the media on 28 October 2009 that the Head of CIPRO, Michael Twum Darko (a foreigner) does not have a security clearance. A request for a security clearance was submitted to NIA in January 2009.

- **Civil Aviation Authority**. The recent (August 2009) theft of pilot examination papers at the Civil Aviation Authority, through obtaining electronic (unauthorised) access, is a further example of the risk associated with ICT fraud/corruption.

In addition to the investigations conducted, further trends established include the following:

- **Intrusive Software Agents** (programmes/applications) as both the vital instrumentality in, and key indicator of, ICTS breaches. Software agents facilitate unauthorised, unobtrusive and remote access to network data, user profiles and passwords. Such access in turn provides a platform for data manipulation (eg fraudulent funds transfers) and the disruption of ICTS. The high prevalence of such software agents was illustrated by the result of a sampled audit at former DFA. All Personal Computers (PCs) sampled were found to contain spyware and remote access software. Similar software was also identified as part of the investigation at DPE.

- The verified and/ or suspected role of **'insiders'** in the breaching of ICTS security integrity at COMSEC and the GSSC serve as examples.

- The involvement of **organised crime** as in some cases criminal syndicates were directly implicated, while in others they were more indirectly instrumental in providing and 'planting' malicious software agents.

- A general tendency of insecure intra-organisational ICTS links to the **Internet**, thus increasing the risk of contamination with intrusive software agents.

- Low level of ICTS security awareness and insufficient adherence to applicable **standards and procedures**.

The NIA investigations cited were prompted by the breaches of ICTS' security integrity for criminal purposes. The deficiencies identified in the course of these investigations raise information security concerns wider than the criminal exploitation thereof for financial gain. These broader concerns should be seen within the context of the twofold interconnectivity of ICTS. Firstly, and similar to most (if not all) other states, the ICTS of government departments and parastatals are part of an interlinked network. The latter in turn is interlinked with the national infrastructural functioning. Secondly, the national ICTS are, to varying degrees, interconnected with the global cyber sphere. Consequently, national and other ICTS could serve as a conduit for espionage, fraud, corruption and related criminal activities and malicious infrastructural disruption.

COMSEC introduced a number of initiatives to address the risks associated with ICT security including the Computer Security Incidence Response Team through which security breaches could be reported electronically. COMSEC also distributed a security needs analysis questionnaire but it has been noted that the response from client institutions are poor.

3. CONCLUSION

It is clear that there are many challenges in improving security in government departments and other client institutions. There remains a need to revisit and evaluate security in prioritised strategic government institutions. One of the initiatives to remedy the situation is the envisaged replacement of the MISS with the National Information Security Regulations (NISR), a crucial development in terms of improving security in the government. The NISR is underpinned by a proper legislative foundation, in terms of the Protection of Information Act, and is intended to address specific deficiencies in the MISS. The NISR will make security measures legally enforceable and set uniform standards to ensure consistency in the government's approach to security matters.

The Protective Security Functional Committee (PSFC) of the CICC recently held a workshop where the mentioned risks and trends have been discussed. All role players agreed to further unpack the aforementioned during the next two meetings of the PSFC meeting. Specific recommendations as to mitigate the risks have also been presented in the annual Departmental Intelligence Estimate.