LUG U MENING

OPROEP OM SKRIFTELIKE VOORLEGGINGS OOR DIE WYSIGINGSWETSONTWERP OP ALGEMENE INTELLIGENSIEWETGEWING [B25-2011]

Die *Ad Hoc*-komitee oor die Wysigingswetsontwerp op Algemene Intelligensiewetgewing (Nasionale Vergadering), nooi belangstellende individue en organisasies om skriftelike voorleggings in te dien oor die Wysigingswetsontwerp op Algemene Intelligensiewetgewing [B25-2011].

Hierdie Wetsontwerp beoog: • die wysiging van die Wet op Nasionale Strategiese Intelligensie, 1994, die Wet op Oorsig van Intelligensiedienste, 1994, en die Wet op Intelligensiedienste, 2002 • die herroeping van die Wet op Elektroniese Kommunikasiesekuriteit (Edms) Bpk., 2002, om sodoende die Staatsekuriteitsagentskap te vestig as 'n liggaam waarin sekere staatskomponente geabsorbeer word • om tegniese veranderings by sekere wette aan te bring wat deur die afskaffing van daardie staatskomponente teweeggebring word • om sekere ander tegniese wysigings aan wette aan te bring, en • om voorsiening te maak vir aangeleenthede wat daarmee verband hou.

Afskrifte van die Wetsontwerp kan verkry word vanaf N. Mbuqe of die Parlementêre webtuiste: www.parliament.gov.za

Skriftelike voorleggings moet gerig word aan Die Sekretaris van die Parlement van die RSA, Posbus 15, Kaapstad 8000, vir aandag me. N. Mbuqe. Tel: 021 403 2793; faks: 021 465 2857 of e-pos: nmbuqe@parliament.gov.za

Die sluitingsdatum is Vrydag, 16 Maart 2012 om 12:00. Openbare aanhore vir dié persone wat vir mondelinge voorleggings gekies word, mag op 27 – 29 Maart 2012 by die Parlement gehou word.

Uitgereik deur: Mnr C.V. Burgess: Voorsitter van die *Ad Hoc*-komitee oor die Wysigingswetsontwerp op Algemene Intelligensiewetgewing.

Parlement. Help ons om Demokrasie te laat werk.

104909

RESTRICTED

P.O. Box 32127
Glenstantia
0010
9 March 2012

The Secretary of Parliament
For the Republic of South Africa
P O Box 15
Cape Town
8000

Attention: Me. N Mbuqe

Ref: "WYSIGINGS WETSONTWERP OP ALGEMENE INTELLIGENSIEWETGEWING [B25-2011]"

If Data and Information can be properly protected;
"why should there be laws to keep it safe?"

Prior to 1994, the research and development for the encryption of data (faxes and telex) (for Government) was done by CSIR, Armscor, SANDF, SAP, Nanotek and the former Department of Foreign Affairs. The body which controlled the Cryptographic environment was the SACSA. Due to the explosion of technological advancement since the nineties and the exponential increase in new and improved technologies, the NCC was born at NIA.

Regarding Nanotek, it has since grown into an industry not only serving Government (the original financiers of Nanotek prior to 1994), but to an industry that also provides services to the Corporate market; e.g. banks.

The achievements of NCC, a very secretive corporation, is unknown.

The latest addition to easy communications was a Smartphone, regarded by many as a safe way of communicating. It has however been proved that all data on this Smartphone's platform flows through computer servers abroad; hence the black out in 2011. Recently it has surfaced that the information/data send via this Smartphone was used in a court case in Canada.

Since Apple's iPad came into use the trend has largely shifted from Smartphone to iPad.

The protection of information has always been regarded by governments worldwide as essential and in the best security interests of a country. During the pre-1994 era, strict emphasis was placed on the protection of sensitive information and the "need to know principle" was strictly enforced. Unfortunately South Africa, once the skunk of the world, became the friend of the world, and a lackadaisical approach surfaced with the notion by many that South Africa has no enemies. This rather peculiar attitude, coupled with a rapidly declining expertise in the field of information classification and security plus the exponential eruption of technological advancement, made historic ways of information protection obsolete and vulnerable to external, unauthorised intrusion.

Due to technological constraints and its exorbitant costs, it was easy in the past to restrict access to certain information and elaborate, but cumbersome systems protected same to the extent that a select few had access to government's sensitive information. The so-called inner circle dealt with the sensitive, classified and often controversial issues. The rest of the public sector staff was mainly

employed to deal with administrative issues, i.e. to ensure rules and regulations were adhered to. After the new government came to power in 1994, the public sector fell into a state of inertia as an amalgamation of the public services of the TBVC states and South Africa took place. Many of the individuals who had no opportunities to join the public service in the past, were also being deployed into senior managerial positions in the newly formed public service of South Africa. At the same time many experienced officials of the former South African public service left the employment of the public sector before a proper exit strategy and succession plan could be established.

This, inevitably, left a void and fertile ground for disruptive forces to exploit the situation. The situation was exacerbated further by the technological advances and accessibility to relatively cheap IT equipment and systems. Unfortunately these advances led to an explosion of information becoming accessible to all in sundry, without any clear policies and guidelines for individuals to adhere to the need to know principle. Access was given to everyone and the duplication/copying/forwarding of information spiralled out of control.

With the introduction of the Bill on the Protection of Information a first step is being taken to revert back to a more acceptable, albeit controversial, level of information protection. It is our view that it will address the symptoms, i.e. what is wrong, but not the root cause of the problem, i.e. why it is a problem.

Given our expertise in the field of information protection and securing it within an ever changing technological environment, it is evident that a paradigm shift is necessary that will ensure the present intolerable leaking and indiscriminate sharing of information to be halted with immediate effect and within acceptable financial means of a Department and the Government.

Problem Defined

- Departmental sensitive information is not secure due to accessibility and defective control mechanisms protecting official information;
- The lack of internal control policies to secure information
- The easy access by everyone to any and, in many instances, all information within departments
- The indiscriminate dissemination of information by everyone
- The ever decreasing cost of information technology and accessibility to it through official and private means increases the proliferation of information by officials
- The easy, inexpensive ownership and accessibility to mass storage devices
- Staff allowed to bring own Laptop/Notebook/iPad/Flashdisk etc to work environment and use it for official purposes
- Freely availability of internet access and previously proliferated information being logically analysed and structured into meaningful knowledge by relatively cheap software
- Freely available internet access to all and sundry
- Private E-mail distribution channels
- Flash disks issued to almost everyone or if not it is cheaply obtainable by individuals in their private capacity
- Flash disk usage by everyone for official and private business concurrently on the same disk
- No system/s available/used to monitor access to information/documents viewed/accessed by whom, when, why, where, etc and if the document/s had been copied/forwarded by whom to whom

- Privately owned IT equipment used by individuals for official purposes – leads to information being stored off site, leading to critical gaps in the departmental data bases and knowledge lapses
- Decision making and/or departmental correspondence may lack credence due to these gaps in the departmental data used
- Information on private computers' hard disks are never erased completely and when computers are sold/phased out the information on the hard disk becomes freely available to the new owner/s who may misuse/sell the information to the media/interested parties
- The fast and easy exchange between private and official IT equipment through e-mails, flash disk usage and even DVD/CD's
- Blackberry/I-Pad/Kindles and other Android cellular phones/apparatus used to send/receive/copy e-mails

Solution

- Access to information must be restricted and the need to know principle must be strictly applied
- All access to departmental information and the copying/distribution thereof must be recorded
- All hardcopies or softcopies made must be registered to identify individual/s accessing and/or copying information
- Departmental information must be categorised and protected according to approved definitions and approved policies with accessing levels established in line with level of security clearance
- The usage of flash disks/clips issued or privately owned must cease with regards to copying/transferring departmental information/documents
- Access to all departmental databases must be controlled and registered
- Access to the internet must be controlled
- Private usage of the internet and private e-mails must be restricted and all e-mails received/sent from any departmental equipment must be recorded on the departmental database with reference also to the sender/receiver and timeframes must be recorded
- Access to the departmental information on data bases must be regulated allowing access only to blocks of information relevant to the duties of an official
- Ignoring any of these guidelines must lead to the withdrawal of an official's security clearance with immediate effect (zero tolerance policy should be in place).

Protection of information must be secured in the shortest possible time. We would like to discuss a solution that is unique, inexpensive and extremely easy to implement that will safeguard against the improper and/or indiscriminate dissemination of information by anyone to a very large extent.

As technology developed, it has become more accessible and affordable. Together with this the indiscriminate access and distribution of public sector information has become the norm rather than the exception. As with the various operating systems when desktop computers and laptops became freely available to everyone, the lack of a uniform policy led to a silo effect and systems were in most cases uniquely applicable only to a specific department. This created compartmentalisation and difficulties to share information among members of the information community. Thus, the "big

picture" was never complete and the gaps in the picture made that many situations were either misunderstood or misinterpreted. The investment in technology and the scarcity of funding also contributed to the unwillingness by some departments to accept a uniformed platform to operate on because a complete refresh of technology would not have been affordable and interoperability seems to gain momentum only at a very slow pace.

Prior to 1994 the departments within the so-called Information Community liaised and shared information on a need to know principle and equipment and training on it was standardised to a large extent. The principle was good, but in essence these departmental systems were developed within the security structures of every department and interoperability was unheard of and simply not acceptable to most departments protecting their own information.

With the establishment of NICOC, coordination improved, but the total picture and uniformity were still not achieved. Unfortunately, with the changes in technology happening at a frightening pace, many of those tasked with the development of policies and the implementation there of, got stuck in what they were used to and new technology has surpassed their level of competency. Due to this and probably the threat of becoming redundant, has led to a state of protecting what is known and unique to a specific environment, rather than accepting change and a uniform system that will be beneficial to the whole of Government. Protection of one's own turf in the technology and information security environment is the first step to ensure fruitless and wasteful expenditure. The value for money principle and economies of scale are also neglected to the detriment of Government.

Uncertainty about the role of previously established coordination committees, e.g. SACSA (SAKSA) to address some of the issues discussed above, has led departments to develop their own policies in this regard. A coordinated approach has fallen away and information sharing and interoperability has become a dream rather than a reality. Furthermore, the tunnel vision by many of the decision makers of what they perceive to be the best, have not been tested and may not be functional or acceptable in all environments. The fact is that globalisation and South Africa's presence in especially Africa, have increased dramatically since 1994 and the technology or systems that may work in a confined area, undoubtedly will not function optimally in all environments. It is therefore imperative that the development of systems and technology that will be used should not be standardised by a Committee of a department and then imposed on others as being the policy of Government.

Due to the inertia in this field and a lack of all the departments to acknowledge/understand the threat, some departments have already proceeded to develop their own policies and procure commercially available equipment/technology, without having these tested in all the environments within which it will be used.

We, therefore, are of the opinion that the cluster of departments that will make use of technology to communicate safely, not only internally, but also internationally and who places a high premium on the protection of information, should establish a competent, coordinating committee that will develop policies and establish uniformed standards that all must adhere to. A Committee will then ensure that a uniform approach will lead to the application of the economies of scale and ultimately the value for money principle will be effective.

Should a body like SITA, SACSA or NCC for instance unilaterally decide to roll out equipment and enforce its will on others based on probably a lack of understanding of the complete environment, it will again lead to a proliferation of systems being implemented by those that have not been consulted beforehand. Equipment that may work perfectly well in a secluded environment, may not be compatible or functional in other environments. In our opinion all equipment that may be used

should be tested under all circumstances and within all environments before a/any decision is taken to deploy same, based on only one organisation's (e.g. SITA, SACSA or NCC) decision. Interoperability and the functioning of all equipment under all different circumstances should be a given to circumvent individuals and remote offices falling back using their private technology rather than intricate and problematic prescribed technology which had not been tested in all environments.

It is therefore of the utmost importance that senior management of all the departments accept and make a decision to once again have a coordinating body, represented by all relevant parties to develop policies and agree on the suitability of uniformed systems rather than having it imposed on all by a single component. This approach of consultation will also bear fruit rather than an approach of high handed confrontation by an individual or single prescriptive organisation.

Yours sincerely

SF Badenhorst
0834548453
fanie@ibhubesi.co.za