Submission to:

The Australian Commonwealth Government
Joint Committee of Public Accounts and Audit

Presented by:

Imperium Technologies of Australia Pty. Ltd.

Inquiry into Management and Integrity of Electronic Information in the Commonwealth

TABLE OF CONTENTS

David Anson
CEO, Imperium Technologies
info@imperiumtechnologies.com.au

TERMS OF REFERENCE

The Committee shall inquire into and report on the potential risks concerning the management and integrity of the Commonwealth's electronic information.

The Commonwealth collects, processes and stores a large amount of private and confidential data about Australians. This information is held by various Commonwealth agencies and private bodies acting on behalf of the Commonwealth. For example, the Australian Taxation Office keeps taxpayer records, the Australian Electoral Commission keeps electoral roll information and Centrelink keeps social security, family and health information. The Committee is concerned that the Commonwealth's electronic information is kept securely and in a manner that ensures its accuracy.

In conducting its inquiry the Committee will consider:

- the privacy, confidentiality and integrity of the Commonwealth's electronic data;
- the management and security of electronic information transmitted by Commonwealth agencies;
- the management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks; and

the adequacy of the current legislative and guidance framework.

SUMMARY

Imperium Technologies welcomes the opportunity to submit to the JCPAA, issues and possible solutions to the management of Electronic Information within the Commonwealth.

Imperium Technologies is the Asia-Pacific provider of secure, open network communication and storage solutions that represent a paradigm shift in the seamless delivery of secure data communication and storage.

The Government of Australia collects, generates and stores information on a myriad of issues and with various security classifications. The information is not centralised but is held by various departments and by external entities that are entrusted to store information on the government's behalf. Issues regarding the storing of this information include:

- **Security** - how secure the information is, both being stored and transmitted?
- **Accountability** - what audit ability is available to account for that information when the information is compromised?
- **Access Control** - who is responsible for the security and ownership of the information?
- **Cost Effectiveness** - how cost effective is it to secure the information and which information is it cost effective to secure?

Due to the complexity and range of electronic information, it is both impractical and unwanted to implement a single storage solution. A solution must offer a risk mitigation strategy that incorporates a combination of policy, procedure and technology to achieve the desired result.

Imperium Technologies utilises products that address the above issues for the transmission and storage of data and are:

- FIPS 140 compliant, making it compliant for U.S., U.K. and Canadian Government use for sensitive but not classified information.
- Multiple Award Schedule Contract Approved for use in the U.S.A by the General Services Administration (G.S.A).
- Compliant with the Administrative Simplification Requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Capable of addressing issues of Security, Accountability, Access Control and Cost Effectiveness.

Imperium Technologies has compiled this document to assist the Australian Commonwealth Government in identifying potential security risks and develop strategies to ensure the integrity of its electronic information and consider worlds best practice policies.

TRENDS IN THE IT SECURITY INDUSTRY

Security of records has always been a concern, both for government and for business. The movement of information from paper based mediums to electronic created greater risk for loss or theft of data as information could be smuggled out on a diskette. This threat later expanded with the growth of the Internet, no longer need a person even remove a physical piece of equipment from a computer, they could send an electronic mail or access systems from their home to gain information. With this increasing functionality came increasing vulnerability, and while external threats are growing at an alarming rate, internal threats still remain one of the most unaddressed, and costly risks that are hard to mitigate.

Current evidence suggests that the possibility of external attack is increasing due to the rising occurrence of cyber attacks against corporations and governments. AusCERT has received 25,197 reports of attempts to compromise Australian computer systems by July 2003, a significant increase from previous years. According to the Australian Institute of Criminology, the use of fraud costs the Australian economy $5.88 billion dollars each year, with much of this being perpetuated through computer systems. The evidence is clear that as more valuable information is stored electronically, there will be increased attempts to access and misuse this information and therefore increased dollar value risk.

It is difficult however to measure the cost of loss of data, and there are several theories as to the real cost for loss of information, it is a hard issue to address, one recent example is where a systems administrator intercepted an electronic mail stating he was to be terminated, and formatted all the companies systems and took their backup tapes with him, the company went bankrupt in less than a month. Recent law changes in California U.S.A. allow for residents of California to be notified if a company they are dealing with, or have dealt with has been breached, no matter how big or small.

The current trend is to develop policies and procedures surrounding existing technologies. Whilst no single solution can solve an organisations security issues, steps can be taken from a policy, procedural and technology standpoint to help mitigate these risks. New technologies and products must be considered and these products should be FIPS 140 accredited products, as this is a recognised best practice standard in cryptography.

FIPS 140 & COMMON CRITERIA

In light of some of the challenges that have been raised earlier during this inquiry, a number of key product certification bodies of major trading partner countries of Australia are outlined below, including a brief overview of their global significance, their various certification policies and how they are addressing similar challenges being addressed by this inquiry.

The National Institute for Science and Technology (NIST) functions includes the following:

1. The United States FIPS 140-1 Cryptographic Module Validation Authority and serves as the issuing and compliance body for Federal Information Processing Standards (FIPS)
2. FIPS Advanced Encryption Standard (AES)
3. Jointly with National Security Agency (NSA) operates the Common Criteria Evaluation and Validation Scheme (CCEVS) under the National Information Assurance Partnership (NIAP), which is the Certification/Validation Body (CB), which issues Common Criteria (CC) Certificates and cooperates as the US representative of the Common Criteria Recognition Arrangement (CCRA).

When there are compelling US Federal Government requirements, such as for security and interoperability, and no acceptable industry solutions exist, NIST issues standards and guidelines for approval by the US Secretary of Commerce. Many of these FIPS are used by federal agencies and have been adopted by industry.

The Communications Security Establishment, Canada (CSE) function includes the following:

1. Canadian FIPS 140-1 Cryptographic Module Validation Authority and serves as the Canadian compliance body for Federal Information Processing Standards (FIPS)
2. Also operates the Canadian Common Criteria Evaluation and Certification Scheme which is the Certification/Validation Body (CB) which issues Common Criteria (CC) Certificates and cooperates as the Canadian representative of the Common Criteria Recognition Arrangement (CCRA).

The Communications-Electronics Security Group (CESG) and the Department of Trade and Industry (DTI) operate the UK IT Security Evaluation and Certification Scheme that is the Certification/Validation Body (CB) which issues Common Criteria (CC) Certificates and cooperates as the UK representative of the Common Criteria Recognition Arrangement (CCRA).

Cryptographic products are graded in terms of three cryptographic protection levels – Baseline, Enhanced and High Grade. Where the required use is for information below RESTRICTED, but still sensitive i.e. PRIVATE, CESG recommends the use of FIPS-140 approved products. FIPS-140 is a US standard that has recently been recognised in the UK and the first UK lab has already been accredited. CESG approved products are issued a certificate detailing the level of cryptographic protection the product offers. The certificate will include the CESG logo.

Results of cryptographic testing can be incorporated into formal CC or ITSEC evaluations.

Overview - SC27 WG3 - Project 19790
Common Criteria standard based on FIPS 140-2 – target date is 2005

IST/33/-/3 is the technical panel that advises the British Standards Institution (BSI) on proposed standards for Information Technology - Security Techniques - Evaluation Criteria for IT Security. It reports to IST/33, the BSI Standards Committee responsible for IT security techniques. IST/33 sets policy and advises BSI how to respond on behalf of the United Kingdom on ballots on proposed European or International Standards.

The Work of IST/33/-/3

IST/33/-/3 tracks the work of an International Standards Working Group - the International Organisation for Standardisation - International Electrotechnical Commission Joint Technical Committee 1 Subcommittee 27 Working Group 3: Security Evaluation Criteria. This is commonly called "SC27 WG3" for short. This WG is responsible for developing standards for IT security evaluation and certification.

The main task of SC 27 WG 3 (and thus IST/33/-/3) has been to produce an ISO/IEC standard corresponding to the "Common Criteria", the large and rather complex IT security evaluation criteria developed by Government agencies in six North American and European Union countries as a replacement for their current national or EEA criteria. The WG3 version of the Common Criteria has now been adopted as an official International Standard, ISO/IEC 15408.

The last meeting of SC 27 WG 3 was in Québec City, Canada, between 28th April and 2nd May 2003.

For many years, WG 3 has concentrated on a limited number of standardisation projects, and recent progress in a number of these areas has been very slow. This last meeting represented something of a change. Three new projects were initiated, dealing with the security assessment of operational systems, security requirements for cryptographic modules and a framework for security evaluation and testing of biometric technologies.

Project 19790, Security Requirements for Cryptographic Modules, is to be based on the recently released US Federal standard FIPS 140-2. Work developing this *standard will be split into two phases. The first phase will "internationalise" the current FIPS standard. The second phase will aim to specify requirements using the language of ISO/IEC 15408 and also address the problems of standardising test processes. The target date for publication of a full International Standard is a challenging November 2005. The first Working Draft is now available.*

The General Services Administration, USA (GSA) is the lead US Government Agency on the e-Authentication initiative, one of two crosscutting initiatives under the US administration's e-government strategy.

The Committee on National Security Systems (CNSS), USA.
NSD 42 specifies the membership of the CNSS. This consists of representatives from 21 U.S. Government Departments and Agencies that are given voting privileges for all CNSS activities. The quarterly meetings of the CNSS are chaired by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. The following are the organizations that have voting membership in the Committee and both Subcommittees:

Department of State
Department of Treasury
Department of Defense
Department of Justice
Department of Commerce
Department of Transportation
Department of Energy
Office of Management and Budget
Central Intelligence Agency
Federal Bureau of Investigation
Federal Emergency Management Agency
General Services Administration
United States Army
United States Navy
United Stated Air Force
United States Marine Corp
National Security Agency
National Communications System
Defense Intelligence Agency
The Joint Chiefs of Staff
Assistant to the President for National Security Affairs

The Committee on National Security Systems (CNSS), USA issued the following policy.

The US Government National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject:

1. National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products was issued by the

National Security Telecommunications and Information Systems Security Committee (NSTISSC), now known as the Committee on National Security Systems (CNSS), in January 2000 and revised in June 2003.

2. The Committee was established by National Security Directive (NSD) No. 42, dated July 1990, and is responsible for developing and promulgating national policies applicable to the security of national security telecommunications and information systems.

3. The CNSS Secretariat can be contacted through the Information Assurance Directorate (IAD) of the National Security Agency (NSA).

NSTISSP No. 11, Revised Fact Sheet
National Information Assurance Acquisition Policy
(Includes deferred compliance guidelines and procedures)
July 2003

Section (below) copied from above Policy Fact Sheet:
(Please see attached NSTISSP 11 revised Fact Sheet.PDF dated July 2003.)

NSTISSP No. 11 also rightfully points out that protection of systems encompasses more than just acquiring the right product. Once acquired, these products must be integrated properly and subject to an accreditation process, which will ensure total integrity of the information and systems to be protected.

Policy

(5) IA shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated GOTS or COTS IA and IA-enabled IT products. These products should provide for the availability of the systems, ensure the integrity and confidentiality of information, and ensure the authentication and non-repudiation of parties in electronic transactions.

(6) On 1 January 2001, preference was to be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) which had been evaluated and validated, as appropriate, in accordance with:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;

- The National Security Agency (NSA) /National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or

- The NIST Federal Information Processing Standard (FIPS) validation program.

(7) Effective 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on the systems specified in paragraph (6), shall be limited only to those which have been evaluated and validated in accordance with the criteria, schemes, or programs specified in the three sub-bullets of paragraph (6).

NIST, CNSS, CSE and CESG (USA, Canada and UK respectively) perform a certification, validation, directive or an advisory role for their respective governments, similarly as Defence Signals Directorate, DSD (representing the Federal Government of Australia) and Government Communications Security Bureau (representing the Government of New Zealand) jointly operate the Australasian Information Security Evaluation Program (AISEP) performs this challenging function in Australia.

Naturally, there are a substantial number of many similar bodies performing similar functions for other governments of major trading partner countries throughout the world. The role they fulfil is both necessary but difficult due to the demanding nature of certifying and advising in relation to these technologies that are highly sophisticated and diverse, yet critical to the security of both the individual citizens and the nation as a whole.

NIST, GSA, CNSS, CSE and CESG as well as other similar bodies recognise, recommend and in some cases mandate Federal Information Processing Standards (FIPS) and/or Common Criteria (CC) certified products.

SC27 WG3 Project 19790 is a WG3 Common Criteria (International Standard, ISO/IEC 15408) project, Security Requirements for Cryptographic Modules, is to be based on the recently released US Federal standard FIPS 140-2.

FIPS PUB 140-1 (Federal Information Processing Standards Publications) specifies the Security Requirements that are to be satisfied by a Cryptographic Module utilised within a security system protecting Sensitive But Unclassified Information (United States) or Designated Information (Canada) within computer and communications systems (including voice systems).

Advanced Encryption Standard (AES) is a Federal Information Processing Standard (FIPS) that specifies a cryptographic algorithm for use by the US Government to protect sensitive (unclassified) information. FIPS Algorithm's such as Rinjdael (AES), Triple-Des (FIPS Cert #114), Skipjack (FIPS Cert #8) and SHA-1 (FIPS Cert #9) are another example of FIPS.

Common Criteria (CC) is an international standard (ISO/IEC Standard 15408) and is an alignment and development of a number of existing European, US and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively) and is over time adopting various FIPS within its framework, as seen in SC27 WG3 Project 19790.

The recognition and acceptance of both FIPS and CC certification by these organisations who are vested with the responsibility to provide guidance to some of the most sophisticated e-Government frameworks being established throughout the globe, such as USA, Canada and UK, is indicative of highly industrialised and technologically advanced trading partners of Australia taking the approach of mutual recognition of both FIPS and CC standards. This thereby ensures the real opportunity of lowest budgetary impact; rapid evaluation capability and streamlined market entry constraints, whilst ensuring the highest security and quality standards are maintained.

Dual certification requirements placed on products (e.g. FIPS and CC) as distinct from a mutual recognition of current recognised global standards has been recognised as an impedance to potential improvements in e-Government security and potentially significant cost savings to Federal Budgets by a number of G8 OECD member countries, and accordingly USA, Canada and UK Governments accept FIPS and/or CC, depending on the individual agency's requirements.

Substantial benefits are potentially delivered to the beneficiaries, such as e-Government frameworks, from appropriate technologies not having to undergo prior to a period of discovery and evaluation, a dual certification (FIPS and CC). An efficient and expedient process of certification recognition and acceptance of recently developed, highly sophisticated solutions offering higher security along with lower TCO may contribute to addressing the same ICT security challenges the Australian Government faces.

In summary, reduction in product evaluation, certification timeframes and reduction of constraints created by duplicated certification requirements have been seriously considered and adopted in other advanced e-Government jurisdictions, and may offer substantial benefits for Australia.

SECURITY PRINCIPLES

Security is not a piece of software, but an entire philosophy. It must incorporate the physical and the technological with precise policy and procedure that allow for global best practice to be adopted.

Many people and organisations recognise the need for security of information, now more than ever. There is a growing awareness in business, government and the public of the need for Electronic Information to be securely stored and transmitted. The major challenge facing all at this stage is how to secure information in a cost effective and efficient manner, whilst not burdening people with a cumbersome difficult to use technology architecture.

In an ideal world, systems such as Public Key Infrastructure (PKI) can be used to secure information both in transit and at rest. The issue that is being faced by security is the fact that the world is far from an ideal. The number of threats to an electronic network is growing daily, both from external and internal sources; disgruntled employees can cause far more damage to an entity than the common hacker who exploits one of the many vulnerabilities that exist in current systems.

The issues facing policy makers today are remarkably different from those faced in the past, and technology advances at an astounding rate. The Information Technology industry is in the process of evolving, particularly in the area of Security. As it does so, new products and technologies emerge that can address some of the issues missed by previous systems. These new technologies however are not the only solution; policy and procedure must play a part in any security implementation and the physical environment cannot be neglected.

A "best effort" approach with restricted administrative access can go a long way to securing electronic information. This “best effort” must be applied to all policy, procedure and the technology and controls implemented from it. There is little purpose in having highly a secure set of policies if one person can with a single phone call bypass all best practice. The “best effort” approach must also be applied to administrators, removing from them the ability to exploit the information and thus also removing from them the burden of responsibility for the information also, this will address the issues of outsourced or off-site redundant information storage.

NEW TECHNOLOGIES IN SECURITY

The future in security is one of systems becoming smarter; these smart systems will be guided by best practice in policy, procedure and technical implementation. Systems that can automatically manage patching, server hardening alert notification and cryptology are the tools that will have the greatest impact on security. In the words of Microsoft's own Security Strategist:

"As computer crime continues to grow, it is increasingly important that companies take steps to protect the security of their data, both in transit and in storage. Although SSL and VPN's have been widely deployed, new products will provide not just secure communications, but will also protect data in storage. Even better, some of these products will produce audit trails, which allow users to track the flow of their data, thus alerting them to any data misuse. Thus, companies concerned with data security will need to carefully consider deploying such products."

Scott Charney,
Formerly: Principal for PWC Cyber crime Prevention and Response Practice,
Currently: Chief Security Strategist for Microsoft

Securit-e-Doc Technology (S-Doc) is at the cutting edge; developed by a team in the U.S. to address the issues that are faced by the use of current technologies. S-Doc provides protection of data both in transit and in storage, with full forensic auditing abilities and based on a Microsoft Windows hardened server platform.

S-Doc technologies include a patented cryptographic engine known as SITT (Secure Information Transport Technology), and smart tools for server hardening and patch management. The SITT engine is capable of utilising server idle time to create ready to use keys for deployment at a moments notice to client systems for use in encrypting and compressing data. This data is then transported directly to the server where the SITT engine manages the storage of the data and upon request sends it to the recipient's machine.

Securit-e-Doc's server based web approach gives a number of advantages, in addition to protection of communications, data in storage and audit capabilities, it also provides an easy to use, rapidly deployed solution that requires no client side software other than a standard web browser.

ISSUES TO BE ADDRESSED

The issues facing the Commonwealth Government of Australia as stated in the introduction are those of Security, Accountability, Access Control and Cost Effectiveness. Each of these issues must be addressed with policy, procedure and technology.

DESCRIPTION OF ISSUES TO BE ADDRESSED

Security of information is of major concern, how secure information is regardless of its classification is an issue that must be considered. Information of a Personal, Non-Corporate nature can be used just as maliciously as Classified Information. Personal information is often used to breach systems. This issue is primarily that of technology, but awareness of security is also a factor that cannot be eliminated here. The issue of security must take into account policy and procedure, identity verification and the need for seamless security.

Accountability for the information contained by the government is one of the major concerns of citizens. The public are aware that the government has both identified and de-identified data about its citizens, and there are real concerns from some areas of the community as to the use of this information. The main way that this can be addressed is through the ability to Audit the information, its flow and usage. This is both a technology and procedural issue; if proper audit controls are in place then the misuse of information is less likely to occur.

Access Control is perhaps one of the hardest issues to address. Administrators all wish to have access to the information for maintenance of it, while varying users have varying needs for access to varying pieces of information. The number of variables here is staggering, and in a large entity such as the Commonwealth Government, the only true way to provide access control is to give ownership to people, and provide those people with a means of controlling the access to the information they own. This issue requires policy, procedure and technology to be implemented as well as an awareness of the possible implications of access to the information.

Cost Effectiveness is one of the major concerns to everyone, if a system is not cost effective, it cannot be widely deployed, and this is often the case with security. Cost effective security is widely regarded as a nice to have, and people compare the cost of accepting a given risk with the effort required to mitigate that risk. What are often not taken into account in security assessment are the intangible or unexpected impacts such as loss of good will, or trust. When intangible benefits are weighed up often it is realised that security is needed, but unaffordable to be deployed so widely to truly mitigate the risk.

ADDRESSING THE ISSUES IN GENERIC TERMS

In generic terms, this section will attempt to provide a view as to how these issues should be approached and addressed without offering any product solution.

The issue of Security is a difficult one to address. Systems such as PKI while able to provide excellent security in an ideal world, are difficult to scale from a small implementation to a large one, and have the added disadvantage of being near impossible to guarantee security. The only way to guarantee the security of PKI systems is to ensure every person in the country who has a PKI certificate and uses it has a completely secure machine, and never loses their certificate. With the theft of computers, PDA and mobile phones increasing as this mobile technology penetrates the community further, this is an impossible task.

Access Control is effectively the ownership and management of data. People must take responsibility for the data they have in their possession. This is not to say that an outsourced company or the IT department who is storing the data has this responsibility, but in actual fact, the clerical staff and the department or company themselves are the owners, and they must control who has access to that data. This access must be managed and audited to ensure correct access.

Accountability must be addressed through the ability to fully audit and track a document from end to end. This cannot be achieved with current technologies such as electronic mail, even if the mail system is enhanced such as in the case of PGP. With this audit ability it will allow easy tracking of access to the data. If a breach occurs to a system that has forensic auditing abilities, the source of the breach can be tracked and action taken.

Cost Effective solutions are those that are scalable and can show proven return on investment (ROI). The challenge here is how you show return on investment for an area that is largely measured in intangible benefits. One method is to assume what is the likelihood of a particular breach occurring, estimate the cost of that breach and determine a dollar factor. When the cumulative dollars for all various breaches are reached even expensive security solutions can show a ROI. This is an issue with no clear answer; it depends on no technology, policy or procedure, but purely on market forces and risk assessment. Increased insurance premiums with legislated risk management premium reductions may be the only way to ensure cost effective security.

ADDRESSING THE ISSUES UTILISING SECURIT-E-DOC

In addressing the above-mentioned issues, one must first consider current technologies as well as those new to the market. Securit-e-Doc's products offer benefits in addressing these issues and can deliver undeniable advantages.

These unique cryptographic products have undergone successful evaluations and are now being adopted or reviewed by a number of Security Conscious Government and Commercial entities in the U.S. and U.K. These products provide highly secure transmission and storage systems, which address the issues encountered not just by the Australian Commonwealth Government, but also by all Governments and Business.

In terms of Security, S-Doc uses recognised cryptography and encrypts each and every document with a unique randomly generated key. This alleviates the need for key management and distribution.

Accountability is addressed through a fully forensic auditable system, which can tell when and where a document was accessed. This audit trail will allow administrators to view data in motion from an administrative view without being able to access the data themselves.

The user in an S-Doc environment manages the Access Control of information. Only the intended recipient can view the data that is being transmitted to them, and administrators can define who is entitled to transmit information to whom. In addition shared folders of information may be established for groups of users.

S-Doc provides a cost-effective security mechanism, with low overheads for management and deployment. The system can be deployed in days and administration and use of the system requires minimal change to your infrastructure. A full end-to-end implementation of PKI for 15,000 users can cost as much as $50 million over a 5-year period and take months to deploy, comparatively S-Doc systems can be as much as one third the price, and can be implemented in a matter of days.

Finally, there is the issue of Interface, the S-Doc technology utilises existing web based interfaces such as Internet Explorer to securely transmit and retrieve information in the form of messages or files. S-Doc is scalable, able to integrate with existing SAN technologies and able to be clustered utilising current Intel and Microsoft Windows Server Technology as its base platform. The easy to use web mail style interface, optional Integrated NTLM or third factor (biometric, smart card) authentication of Securit-e-Vault and the customisable interface available with Securit-e-API gives the ability to manage sensitive but not classified data and access it anywhere, anytime it is needed.

SITT TECHNOLOGY OVERVIEW

Secure Information Transport Technology (SITT) offers a seamless method of managing cryptography. The system uses either software or hardware based Random Number Generator (RNG) to issue unique keys for each and every transaction, the software itself then performs the management of those keys. This managed approach combined with the Interactive Hypertext Marked Language (IHTML) delivery functions that utilise Active-X or Java components allows for seamless key management.

The SITT engine does more than this; it also manages the data store, which consists of a number of areas, and is very simple to manage. The data store contains the account details, audit logs and of course the data itself, this is all kept encrypted and can be placed on any or multiple file share(s) with a point and click management interface.

SITT uses a standard web browser with SSL connection to protect login details and through use of the Securit-e-API's can be placed into any existing web application, such as internet banking, online shopping or even government records retrieval to provide a secure method of transferring documents to a client system.

CONCLUSION

Security of Electronic Information is an issue of key importance to Government, Business and the Information Technology Industry. Imperium Technologies advocates the use of tools that are beneficial to the management of electronic information security. Tools however are only as good as the procedures and policies that are implemented with them, and there is still a need for products such as Anti-Virus, Firewalls and PKI.

What we do advocate is that for information that is Sensitive, but not classified, solutions other than that of Gatekeeper can be of benefit to not just the Australian Commonwealth Government, but the people of Australia, through the protection and accountability for their data.

The conclusion that can be drawn from this is that Securit-e-Doc and Imperium Technologies have a set of products that is cost effective, secure, user friendly, versatile, auditable, has user driven access control, web based, easy to deploy and administer, and finally that can deliver encryption to you when and where needed **a true end-to-end solution**.

David Anson
CEO, Imperium Technologies

ADDENDUMS

ADDENDUM A – Securit-e-Vault Whitepaper

Securit-e-Vault™ Technical Overview - Whitepaper

Securit-e-Vault™ software enables the secure transport of electronic files and messages via the Internet or an intranet with the additional protection of that data while stored on a highly secure Web server. Securit-e-Vault's vast feature set provides end users a secure alternative method for conventional e-mail attachment communication, a secure Web-based method of moving large data files, a secure replacement for standard FTP server transport, and a secure message delivery system. Critical data stored on a Securit-e-Vault server remains protected at all times by automated, transparent encryption and compression. Only authorized users can access stored data with appropriate login information, including an optional second factor capability for access control.

Securit-e-Vault is server-based software that operates with an easy-to-use interface for both administrators and end users. Using an online key registration system, the software is installed on a server using a particular Web domain and is accessed by a preset URL address (e.g., the Securit-e-Vault application would operate under IIS 4.0+, within a domain on a Microsoft® Windows® NT or 2000 server). After a successful secure login, authenticated users transport or retrieve files and/or messages from their client computer to the Securit-e-Vault application data store via a Web-based interface. In addition, all administrative functions are Web-based through the application's interactive interface system. Access permissions are established at the start of any transaction by the sender, determining intended recipient(s). All recipients must have user accounts within that Securit-e-Vault system in order to transport or retrieve files or messages.

Based on specific user permissions and quotas, files or messages can be optionally transported to specific intended recipients, to a central archive storage area for groups, or to a personal user storage area – all via that particular Securit-e-Vault server.

The system utilizes standard SSL transport protocol to ensure a secure, authenticated session between the Securit-e-Vault server and a Web browser. Further, data is additionally encrypted on the client-side, prior to server transport and storage, by a one-time-use symmetric encryption applet or object delivered automatically from the server to the client computer. The Java-based applet or ActiveX object is delivered dynamically by the server as a real-time plug-in to the requesting client-side Web browser. Upon completion of a transport or retrieval transaction, the plug-in and any critical associated data is deleted from the client computer.

The closed cryptosystem, known as SITT® (Secure Information Transport Technology), delivers an encryption algorithm, in particular Triple DES, Skipjack or Rinjdael (AES) at a key length of 196, 96 and 128 bits, respectively. The encryption algorithm, chosen at the time of system installation, is seeded using a standard hardware white noise generator or pseudo algorithm supplied to generate the unique encryption key for each and every transaction. The encryption key is delivered directly to the client/browser plug-in using a secure, encrypted key exchange process. The SITT cryptosystem enables secure storage of files or messages on a server using a fully automated and transparent, secure key management system. The key manager and highly detailed audit log system use the same level and type of encryption as above. No client-side software is required, other than a properly configured Web browser (i.e., Internet Explorer or Netscape®) to transport or retrieve encrypted data files or messages, making for simple deployment of the platform. Data protection is maximized in this manner as the information is protected at its "point-of-origin" and remains well protected (using multiple layers of encryption) during both transport and storage. The point-of-origin, automated encryption eliminates the dependency on VPN (Virtual Private Network) or PKI (Public Key Infrastructure) systems to ensure the security of both data-in-motion and data-at-rest on the server. The fully encrypted file system, managed completely by the application, maintains the security and integrity of all stored information within the Securit-e-Vault system.

Optionally, an e-mail notification message that a file or message has been transported and is awaiting retrieval can be dispatched to the intended recipient(s) by the Securit-e-Vault system. This automated, standard SMTP e-mail notification simplifies user retrieval of any secure files or messages. By providing a direct hyperlink in an e-mail message for the recipient to select for direct access to the sending Securit-e-Vault system, an authorized recipient, through almost any connected Web browser, can easily retrieve the secure information. Additional features include a comprehensive file/folder management system, allowing users to search and organize their personal storage area within the secure Securit-e-Vault encrypted file system. The Securit-e- Vault system provides users the overall capability of audited communication and collaboration that includes proof of delivery via the Internet or an intranet, with total portability and complete privacy. Granular, Web-based system administration as well as user access simplifies both deployment and total rights management.

Securit-e-Vault, using SITT's complete automation and transparent encryption delivery engine, minimizes the need for extensive IT resources to ensure a secure, virtual communication and data storage platform. Securit-e-Vault, designed as an intelligent software application with respect to security, acts as a complete end-to-end, secure communication and collaboration platform that leverages the capabilities of most any network connected Web browser. Beyond the scope of conventional email, Securit-e-Vault empowers us with the ability to securely monitor, track and manage information flow and digital rights using almost any open network, including the Internet, as its platform.

ADDENDUM B – CNSS Fact Sheet

See attached: NSTISSP 11 revised Fact Sheet.pdf