AUSTRALIAN
CUSTOMS SERVICE

SUBMISSION TO THE JOINT COMMITTEE ON PUBLIC ACCOUNTS AND AUDIT – INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

10 January 2003

10 January 2003

SUBMISSION TO THE JOINT COMMITTEE ON PUBLIC ACCOUNTS AND AUDIT – INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

CONTENTS

SUBMISSION TO THE JOINT COMMITTEE ON PUBLIC ACCOUNTS AND AUDIT – INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

Executive Summary

Customs manages the security and integrity of Australia's borders. To perform this role Customs receives, processes and stores large volumes of information electronically on the movement of all goods and travellers crossing Australia's borders. In collecting and acting on this information Customs works closely with other agencies with whom it has electronic connections through which limited information is passed.

Much of the information held by Customs is of a sensitive or private nature and Customs therefore has taken extensive precautions to assure the integrity, security and confidentiality of its electronic communications and data holdings.

These precautions include specific requirements placed on Customs IT service provider, EDS, to physically separate and secure Customs infrastructure and to protect its networks and data holdings against attack. It also includes regular audits and inspections to ensure the physical security of its infrastructure.

Given the sensitivity of information held by Customs, with few exceptions, data holdings and applications are also separated from external open systems such as the Internet. In general, communications with Customs applications from the external environment are "mediated" by downloading or processing information from transmissions before it is passed to a Customs application.

Customs management regime for assuring integrity and confidentiality is rigorous. Severe penalties established in legislation for unauthorised disclosure of information applies equally to Customs personnel and its service providers. A tightly controlled regime for authorised information disclosure is well established. Access controls for Customs personnel apply on a "need to know" basis. External users are subject to a detailed registration process and can only access copies of their own information. Extensive logging, backups and disaster recovery plans are in place to manage integrity and redress failure.

An area of immediate challenge for Customs is with the adoption of Public Key Infrastructure (PKI). Consistent with the government's Gatekeeper strategy, PKI is being adopted as the means for assuring the identity and integrity of communication within open environments such as the Internet. PKI offers strong assurance of the integrity of message content. However, the means by which an individual's identity is certified to be true at the time of issuing a certificate is less certain. To address this, Customs is enhancing the Evidence of Identity requirements under the points system of the *Financial Transactions and Reports Act 1988* and consistent with the

Gatekeeper strategy. However, the development of individually tailored agency requirements potentially limits the interoperability of digital certificates. Customs therefore supports a national approach to resolution of this matter.

Introduction

This submission focuses on measures Customs takes, now and into the future, to assure the security and integrity of the electronic information it receives, processes and holds.

Customs submission is directed at its major information holdings and transmissions and the steps taken to protect the security, integrity and confidentiality of those holdings and transmissions. This submission also focuses on the principles that Customs adopts in this regard. The submission is therefore not intended to address all elements and details of Customs information management.

Two areas of particular interest discussed in this submission are the arrangements needed for establishing these assurances within an outsourced IT environment and the emerging issues in assuring the identity of those communicating within open environments such as the internet.

While security and management arrangements with IT service providers are now well tested and proven, the emerging issues in identity are a new challenge within electronic information management and an area of topical debate. Customs, as an early adopter of Public Key Infrastructure (PKI), is in the process of establishing and testing its approach to strengthening the assurance of identity and some of the issues faced so far are included in this submission.

Customs Role and The Need for Security, Integrity and Confidentiality

Customs manages the security and integrity of Australia's borders. It works closely with other Government agencies and international organisations to detect and deter unlawful movement of goods and people across the Australian border.

To achieve this, Customs operates as a national organisation and collects, stores and processes a wide range of information about travellers and goods. In 2001-02 financial year alone approximately 5.55 million consignments and around 17 million travellers were processed [1]. The overwhelming majority of information associated with these movements was processed and stored electronically.

[1] Australian Customs Service Annual Report 2001-2002 page 8

The use of electronic processing is essential given the scale of Customs operation and important in ensuring that it achieves two of its primary roles, namely:

- to facilitate trade and movement of people across the Australian border while protecting the community and maintaining appropriate compliance with Australian law:
- to efficiently collect customs revenue.[2]

Much of the information Customs receives is either commercially sensitive or private in nature and therefore requires relatively high levels of security and probity in its management. The information is used to make decisions about:

- clearances or approvals that may be granted;
- revenues that might be collected;
- penalties or investigations to be pursued under the various legislation administered by Customs.

In collecting and acting on the information received, Customs works closely with other organisations, including the Australian Quarantine and Inspection Service (AQIS) and the Department of Immigration Multicultural and Indigenous Affairs (DIMIA) with whom electronic connections are maintained for processing goods and travellers.

Compromises in the integrity, confidentiality or privacy of the information Customs holds, or the communication processes by which information is received, clearly challenge the underpinnings of Customs operations, the confidence that can be had in the organisation and the strength of its decisions. For this reason, Customs has placed a high importance on assuring the governance, technology and legal framework surrounding its information management and communication systems.

Customs Information Holdings

Customs electronic information holdings largely involve data relating to the movement of travellers and goods into and out of Australia.

With respect to travellers, data is received and held on all those entering or leaving the country, including crew members. This information includes the details of each person travelling (name, date of birth, sex, nationality and travel document number), and may include information on goods they are known to be carrying that are prohibited, require action by AQIS or that may attract a duty. This information may also be used to identify potential threats to the community such as those persons likely to be involved in illicit trade or terrorist activity. Passport information on passengers is received electronically from airline and cruise companies and provided electronically to DIMIA, on whose behalf Customs acts.

[2] Extract from Custom corporate vision, *Australian Customs Service Annual Report 2002*

The vast majority of electronic information received and held on the movement of goods relates to import and export declarations and the reporting of consignments prior to their release into or out of the country. The systems that support these functions are connected with AQIS. This connection is used to coordinate clearance of goods where a consignment requires a quarantine permit. Information held includes the details of owners and their goods, their agents, transportation arrangements and the origin and destination of goods. This information is used to assess and collect Customs revenue as well as to identify the risk to the community that particular consignments may present.

Customs Information Systems

The Changing Context

Customs was amongst the first Government agencies to adopt electronic receipt, processing and storage of data. As early as 1972 Customs implemented the first automated import entry system in the world.[3] The success of this first application led to its replacement in 1976 with a more interactive approach allowing clients to make their own electronic entries through purchase of a dedicated line[4]. Over some thirty years Customs has developed electronic systems, becoming a leader in the use and application of Electronic Data Interchange (EDI) and encouraging the uptake of electronic commerce methodologies by the logistics industry as well as importers and exporters.

During this period Customs faced many of the issues that confront all agencies in deciding to transact electronically. For example, the development of user and confidentiality agreements, management of identity and evidentiary trails (i.e. logs and transaction records) as well as archive and security practices for information held.

Many of the Customs systems that developed between 1972 and 1993 are reaching the limits of their capacity and are rapidly being overtaken by recent technology advances and the reducing cost of transacting within an open (i.e. internet based) environment. This challenge is being addressed under the Cargo Management Re-engineering project (CMR)[5]. This project involves the integration and re-design of Customs commercial programs that deal with the movement of goods as well as the development of the Customs Connect Facility (CCF) for communicating electronically with Customs. This project will allow for: the integration of Customs commercial transaction base and the associated data bases; development of a new client registration system; greater access to transacting with Customs on-line through

[3] This system was called INSPECT and involved data input by Customs own operatives.

[4] This was COMPILE 1. COMPILE stands for Customs Online Method of Preparing from Invoices Lodgeable Entries. While relatively simple in 1976, the system has been progressively enhanced to include facilities for electronic funds transfer to pay duties.

[5] www.customs.gov.au contains extensive information on the CMR project.

internet based communications; and the application of Public Key Infrastructure (PKI). These changes are discussed in more detail below.

The Technical Environment – Physical Security

Internal Environment

One of the greatest threats to the security and integrity of electronic information is the connection that may exist between internal systems and the external world. Open systems are most vulnerable to attack (and possible compromise of the integrity of data holdings) by outside sources since they involve external access into an organisation's information holdings and applications. Closed systems, on the other hand, rely on some form of mediation between the external world and an organisation's systems, but do not involve direct access to the holdings or applications supporting those holdings.

Given the sensitivity of information held by Customs, a conscious decision has been made to maintain data holdings and applications within closed systems and to effectively isolate the technical operation of those systems from other organisations and networks. This concern is a significant factor in considering options for establishing Internet connection through the Local Area Networks (LAN).

This high importance Customs assigns to the security of its systems and data holdings can be seen at all levels of Customs IT systems.

At the level of physical security, for example, Customs has specified to its IT service provider (EDS) that its system "boxes" must be housed in separate enclosures and secured from that of other operations. Premises where data is stored must be secured to a T4 endorsed standard under the Protective Security Manual 2000 and as recommended by Defence Signals Directorate. In an outsourced environment this is a particularly important requirement since it is common practice for service providers to co-host their client systems and use "logical" barriers to separate them. In delivering these services, EDS maintains a secure facility within the computing centre in which physically separate machines and communication channels are dedicated to Customs. The security surrounding the Customs section of the EDS facility is managed to a Highly Protected level with coded access, record of access and surveillance being maintained.

Customs major applications that receive information on trade and travel are housed on these separate and secured machines and direct electronic access can only be gained internally via secured LANs.

Customs maintains a discipline of risk assessment and risk management in the design and implementation of its systems to determine and redress points of failure, weaknesses in serviceability and vulnerability to attack. Customs also has a disaster recovery plan which it maintains as an on-going project. The planning process is intended to be all embracing and addresses recovery of services and data from malicious cyber or physical attack through to operational failures.

External Connection to Customs

Major Applications

While Customs favours closed systems separated from those of other organisations, it does have extensive facilities for the transmission and receipt of electronic information.

A number of Customs applications receive and process information from clients and provide responses to confirm messages or to provide outcomes of decisions. Customs commercial applications that deal with the import and export of goods are a case in point. These systems do not, however, allow clients to communicate directly with the databases or the applications. COMPILE[6], the oldest of Customs existing commercial systems, is an exception where identified and traceable clients do have a direct connection to the application to create their own records, but do not have direct access to the database. For other commercial applications, the information is transmitted using EDI and is then imported into the relevant Customs system.

The same approach is being taken with the Integrated Cargo Systems (ICS) being built under the Cargo Management Re-engineering project. Communication will be managed via the Customs Connect Facility (CCF), a secure gateway. The ICS will replace all commercial cargo systems, including COMPILE. The CCF will allow for messages to be received and sent using the Internet as a carriage. Clients will be able to interact through this gateway in "real time," however, the information they provide will be processed from their communication and passed into the ICS.

Desktop Communications

Customs systems can be accessed directly by authorised Customs personnel via a Customs LAN. These LANs receive and transmit e-mails and in this they can be said to have limited connection to an "open" external environment. Extensive precautions have been taken in this regard to ensure the integrity and security of the e-mail system. In-coming and out-going messages, for example, are transmitted through a communication backbone in the Government's Secure Gateway Environment (SGE) shared with other agencies. To ensure separation from other agencies and to protect the integrity of the message, all Customs data is encrypted prior to entering and after leaving the "backbone" using encryption equivalent to a security level of Highly Protected.

In addition to these steps, multiple levels of virus protection are used at each firewall through which the messages pass. One level deals with messages entering the SGE,

[6] In addition to the direct access noted above, COMPILE can be communicated with using EDI.

another deals with messages leaving the SGE and then entering the Customs network down to the desktop level. Virus profiles are updated on receipt from the vendor. The firewalls in combination with access limitations and procedures (discussed at various points below) also serve to detect and frustrate hacking attempts.

E-mail communications with other agencies requiring "In-confidence" transmission or above are transmitted through a Virtual Private Network (VPN) within the SGE. Customs has also installed a second firewall within its network to provide a Secure Enclave. This is used for transmitting messages at up to a "highly protected" level within Customs and with other agencies. As with other Customs applications within the Customs network, this is not accessible to all Customs officers. In addition to the requisite security clearance, they must hold a position for which such access is required for their work.

Managing Integrity, Confidentiality and Privacy

Internal Management

Regardless of the strength of an agency's physical or technical security, a management regime is essential to assure the appropriate actions and vigilance of those using and supporting the systems. Customs operates to a number of principles in this regard including:

- assuring the integrity of all those acting in its interest;
- operating on a "need to know basis";
- access to only your own data; and
- assuring the identity of those with whom it deals.

Section 16 Customs Administration Act 1985

Customs makes no distinctions between the responsibilities and obligations applying to the paper, spoken or electronic systems. At the head of its measures is Section 16 of the *Customs Administration Act 1985*. This provision is broad in scope and applies to anybody employed by, acting or providing services for Customs.

Section 16 prohibits the unauthorised recording and disclosure of information held by Customs. In addition it makes specific protection with regard to personal information, as defined by the *Privacy Act 1988* and serves to complement the application of that Act within the Customs context. Penalties of a two-year prison sentence can be imposed where an individual is found to be in breach of this provision. Section 16 also establishes the basis on which information may be disclosed. Under a system of delegation, this usually involves prescriptions that limit the disclosure to specified positions, purposes, entities and forms of disclosure.

All staff and contractors, including EDS staff, are made aware of the non-disclosure provisions of Section 16, and the consequences of any breach, as part of induction. They are also required to sign an acknowledgement to this effect. Awareness of the security environment, procedures and obligations are updated with regular and compulsory security training.

Access to Information and Facilities

Customs has imposed strict requirements on its IT service provider, EDS. All EDS staff must, as with Customs staff, be security cleared to a “Protected” level. EDS staff involved in the management of systems that hold Customs data require security clearance to a level of “Highly Protected”. Potential breaches of Customs security requirements by EDS can involve termination of employment.

Security procedures have also been put in place to minimise the risk of compromise to Customs systems. This includes a requirement for no less than two staff to be present when access is made to any T4 (Highly Protected) areas where Customs systems are housed. It also includes a requirement for any third party to be accompanied at all times by those already authorised for access.

Compliance with Customs requirements is assured both through EDS’s own corporate arrangements as well as through audits and site examinations by Customs IT security personnel. Any issues that may arise, in this or other areas of delivery by EDS, are managed through an established process of escalation at peer level within both organisations and regular management meetings at which performance is reviewed and monitored.

While all Customs staff are cleared to a “Protected” level or above, they cannot access all protected material. Access is limited to information that corresponds to the duties they perform. This is effected through an access policy designed to minimise the risk of unauthorised access. Access is linked to the user’s identity which is used in combination with their password when accessing the network. Customs applications, other than the more commonly required packages such as e-mail and word-processing, require a separate level of authorisation and separate password also linked to the officer’s user-id. Where authority is not provided for access, the application and its functions are not displayed. Passwords are audited to ensure that they cannot be easily cracked and continuously refreshed with a limitation on the re-use of former passwords.

Integrity of Data

The integrity of information holdings is supported by extensive audit logs that record changes in data, the time of changes and person making the change. In addition, a thorough process of daily backups is used along with a remote disaster recovery facility for data held on Customs systems. A significant improvement in the logging and management of changed records will be effected once the new Integrated Cargo System (ICS) is implemented. With this new system no business data will be overwritten, instead the old record is closed and a new record inserted. This approach ensures that the integrity of the data can be readily established regardless of the frequency with which backups are performed.

Customs also takes extensive precautions in the disposal of electronic records. Records are retained for minimum periods designated under relevant laws, including the *Archives Act 1983* and the Customs legislation. Records are reviewed prior to disposal to ensure that they are not subject to current action and that disposal would comply with the laws relating to retention of records. The final disposal of all redundant records and hardware storage units is carried out in accordance with the requirements set down by Defence Signals Directorate (DSD). This will vary from simple de-gaussing[7] in the case of In-Confidence records through to complete destruction of hardware (e.g. incineration of the storage medium) where it once hosted records rated at a level of Protected and above.

Assurance of Privacy

The strategies employed to assure confidentiality, security and integrity of data also act to assure the privacy of individuals to whom the data may relate. Under these strategies, for example, data is only accessed by those with appropriate security classification and who hold a role that requires them to act on the information. This is consistent with the principle and practice that information is only accessed for the disclosed purpose for which it is collected.

Customs management of passenger information it receives electronically is illustrative of this. Customs is able to access passenger information from airlines to enable it to fulfil its statutory functions. Passengers are advised that Customs may access personal information and are advised of the purposes for which the information will be used. Information collected only for Customs purposes is not transmitted to any other agency unless the disclosure is authorised under section 16 of the *Customs Administration Act* and as with all other Customs systems, only Customs staff with both the appropriate security classification and holding a designated position for access are able to view the information. In other circumstances, where Customs collects information on behalf of other agencies such as DIMIA, the information is passed on to those agencies electronically and is only retained by Customs for a limited period.

Managing External Clients

Those providing information to Customs present a different information management challenge to the internal user or service provider. Most information received by Customs is from businesses, whether it be from airlines providing passenger data or Customs brokers providing import and export declarations. Generally Customs would have had prior dealings with a business and would be familiar with its operations and its personnel.

[7] De-gaussing is a process for destroying the digitally stored information by use of a magnetic field.

Registration of External Clients

For an external client to communicate with a Customs system, they first need to go through a registration process. Under the present commercial systems, this involves making application to Customs, gaining Customs approval and agreeing to a set of user terms and conditions before an access code will be provided. In fact, for the Customs commercial systems such as COMPILE this process is specified in the *Customs Act 1901.*[8]

Access Limitations

As with internal users, external users are limited in their access to Customs systems. One limitation that always exists for an external user is that a user can only access records of information that they input, or that was input within the limitation imposed by their own organisation's structure. This is a significant security and privacy consideration. Other limitations are assigned using the Remote Access Control Facility (RACF). This facility contains a list of application resources relating to creation, reading, updating, deletion, execution and printing functions which must be specifically requested and assigned. This facility not only provides Customs with a control over access but allows clients to determine governance arrangements with respect to their own access.

With the introduction of the Customs Connect Facility (CCF) this year, an electronic client registration system will be introduced. This will operate hand in hand with the Public Key Infrastructure (see ***The Challenge of Identity*** below). The registration system will define the access rights that each user may have to the system while the secure perimeter[9] prevents users from accessing other aspects of the Customs network. In supporting this, the CCF will add at least 6 additional firewalls into the communication chain and will act to protect the systems to which it is linked against hacking and other forms of attack. As with other interfaces, the secured perimeter will undergo penetration testing by an independent third party to standards set down by the DSD.

The Challenge of Identity

Customs is soon to implement Public Key Infrastructure (PKI) based on the Government's Gatekeeper[10] framework to provide non-repudiation of content and assurance of identity. PKI will be used to identify those communicating through the new gateway (CCF) and to assure the integrity of their message. This process will

[8] *Custom Act 1901* Section 77A prescribes the means of registration for COMPILE, the import declaration system, and Section 122A prescribes the arrangements for EXIT, the export declaration system.

[9] Secure perimeter refers to the IT security cordon that surrounds the point of entry for electronic communications.

[10] Gatekeeper is a Commonwealth Government initiative providing a framework for Public Key Infrastructure. It involves a rigorous accreditation scheme for organisations and service providers wishing to issue digital certification. For details see www.noie.gov.au.

initially be used in connection with the new Integrated Cargo System (ICS) but can logically be extended to other applications. This will mark a departure from relying entirely on closed systems and Customs current role in registering its users. In future, instead of making formal application to Customs to access its systems, clients will be able to present a valid electronic certificate and go through an on-line registration process for use and access. This has involved changes in Customs legislation with the introduction of the *Customs Legislation Amendment and Repeal (International Trade Modernisation) Act 2001.*

These certificates will likely be obtained from an independent Certifying Authority whose Registration Authority attests to the holder's identity. All messages would be encrypted and linked irrevocably to the certificate.

This approach is an important initiative in broadening the access to Customs systems, meeting the Government's on-line objectives and in taking advantage of Internet based communications with clients. PKI will offer a high level of integrity in the information transmitted to and from Customs because it not only encrypts the information but produces an algorithm able to validate that nothing has altered during transmission. It also clearly links the content to a digital certificate used to identify the sender. However, despite the strength of security and integrity offered at the technical level under PKI, there are certain challenges in the management of PKI that relate to the certainty one can have as to the true identity of the certificate owner.

The principal challenge has been in the area of evidence of identity (EoI). Declarations and other statements made to Customs are used to assess risk to the community and may also be used in evidence where a breach of statutory requirements might lead to prosecution. In this environment there needs to be a high level of non-repudiation between an individual or business and the representations they make under the Customs legislation such as binding declarations for import and export of goods. Where this connection is weakened, the integrity of information received is compromised because it cannot be correctly attributed to the sender.

The standard normally used for EoI is drawn from regulations under the *Financial Transactions and Reports Act 1988* (FTRA) establishing the 50, 100 and 150 points check. Certificates generally available in the market place, including Gatekeeper compliant certificates, assume points systems in their pricing for certificates. However there are weaknesses with this system since it is possible to establish a proof of identity without a clear link between an individual's physical identity (a picture), their address and their physical signature.

Customs intends to address this by enhancing its requirements within the overall auspices of the FTRA points system and consistent with the Gatekeeper strategy. This includes the production to an authority certifying the identity of at least one document with a current residential address, a recognisable photograph, and the date of birth and signature along with the individual's name being on all documents presented.

The development of individually tailored agency requirements potentially limits the interoperability of digital certificates. Customs does see benefit in considering a more national approach to the issue of EoI in order to reduce the overall cost to and burden on the certificate holder and overall raise the standard of validation of identity. In this regard, Customs notes that the Attorney-General's Department has been considering EoI from a policy perspective.

Conclusion

The security and integrity of information management continues to be a matter of high importance to Customs. The approaches outlined in this submission governing both internal security and protection regimes as well as stringent conditions imposed upon external service providers are strong indicators of corporate commitment to the proper management of public information.

Along with many other agencies, Customs faces the challenges of operating in an open environment through the development of strategies aimed at taking full advantage of the new environment while not compromising security, confidentiality or integrity. The key strategy that Customs is employing is to maintain closed internal systems for information holdings and applications in tandem with secured communication within the open environment.

Further challenges exist in the matter of assuring identity in the open environment we now face. As one of the first Commonwealth agencies to embrace PKI, Customs has made significant progress in terms of resolving many of the difficulties within its own operating context.

Peter Naylor
National Manager Information Management
10 January 2003