Defence Signals Directorate
Information Security Group
Locked Bag 5076
KINGSTON ACT 2604

Ph: +61 2 6265-0197
Fax: +61 2 6265-0328

DSD 2002/1734
ASQ 143/03

Mr Tas Luttrell
Inquiry Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Mr Lutrell

ADDITIONAL BRIEFING MATERIAL – INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

We undertook during the Directorate's public appearance before the Committee in June to provide some additional information relating to our role in product evaluations and some additional comments on Fedlink and other Virtual Private Networks.

Attached please find two papers, release of which has been approved by the Minister for Defence. I hope they answer the residual questions that committee members had. I am also providing electronic copies separately via email.

In addition I am enclosing some documents that outline in greater detail the Common Criteria standard and the Australasian Information Security Evaluation Program, which DSD runs.

If you require any additional information or clarification, please let me know. I can be reached on 02 6265-0323.

Yours sincerely

[signed]

Tim Burmeister
A/AS Information Security

July 2003

Enclosures:

1. The Australasian Information Security Evaluation Program
2. Virtual Private Networks
3. Three AISEP and Common Criteria explanatory documents (8 copies of each)

CC: DepSec Intelligence and Security
Inspector-General of Defence
Assistant Secretary, Ministerial Support and Defence Governance

Defence Signals Directorate
Information Security Group
Locked Bag 5076
KINGSTON ACT 2604

Ph: +61 2 6265-0197
Fax: +61 2 6265-0328

THE AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

The aim of this document is to provide supplementary information regarding the operation of the *Australasian Information Security Evaluation Program* (AISEP) following the Defence Signal Directorate's (DSD) public appearance before the Joint Committee of Public Accounts and Audit review of the management and integrity of electronic information in the Commonwealth on 16 June 2003.

Three main areas are addressed: the nature of the evaluation and certification process itself; the potential for conflict of interest between companies operating evaluation facilities and their competitors in other areas of IT services and products; and the cost and duration of the evaluation process.

THE EVALUATION AND CERTIFICATION PROCESS

These comments pertain to Senator Lundy's query regarding the actual evaluation and certification procedures as conducted under the AISEP.

Essentially there are three phases to the evaluation/certification process:

- ***Pre-evaluation***: Depending on their level of evaluation experience and knowledge, a developer will normally work with a pre-evaluation consultant before entering a product into evaluation. The main activities in this phase are to:
  - define the Target of Evaluation, which is the IT product or system to be evaluated (including associated guidance and documentation); and
  - develop the Security Target, which is the formal statement of the product's security claims (against which it will be assessed).

  Pre-evaluation services may be provided by the licenced evaluation facilities (though other providers exist) but must not be undertaken by staff who will subsequently be involved in the evaluation. During this phase DSD will assess the suitability of the Target of Evaluation and Security Target – both from the standpoint of technical correctness and adherence to Government IT security policy – and conduct an initial review of any cryptographic functionality.
- ***Evaluation****:* The evaluation itself is a formal, structured process carried out by the evaluation facilities in accordance with the work units and methodology prescribed in the Common Criteria and Common Evaluation Methodology. DSD has responsibility for oversight of the evaluation through:
  - observation of testing procedures;
  - delivery of work package reports; and
  - regular technical interaction and progress meetings with evaluation facility staff.

  DSD also performs any cryptographic evaluation that may be required in parallel with the evaluation by the commercial facility. At the conclusion of the evaluation, the facility provides DSD with an Evaluation Technical Report.
- ***Certification***: In the final phase DSD reviews the Evaluation Technical Report as a final check on the technical correctness of the evaluation and the validity of the results. DSD then prepares a summarized version of this (minus any proprietary information) known as the Certification Report, and issues a Certificate stating that the Target of Evaluation meets the claimed assurance level. The Certification Report, together with the Security Target, are made available on the product's entry on the Evaluated Products List on the DSD website.

More detailed information on the various components of an evaluation, should they be required, can be found in the attached *Common Criteria User Guide.*

POTENTIAL FOR CONFLICT OF INTEREST

Senator Lundy also raised a number of questions regarding the potential for conflict of interest where companies which operate evaluation facilities also provide products or services which are in competition with products entered for evaluation.

The three currently licenced evaluation facilities have never formally raised a conflict of interest issue with DSD. This is probably due primarily to the stringent conflict of interest provisions which are contained in the licence agreements under which each of the facilities is obliged to operate. Apart from the requirement (which was stated at DSD's JCPAA appearance) that an Australasian Information Security Evaluation Facility must operate "as a separate entity from its parent company, if any, and any other party", the following specific conditions apply with respect to conflict of interest.

4.1 Conflict of Interest

4.1.1 The AISEF or any employee of the AISEF involved in a Security Evaluation shall not have any commercial, financial, personal or other interest in the outcome of the Security Evaluation.

4.1.2 Without limiting the generality of paragraph 4.1.1 the AISEF shall be deemed to have a commercial interest in the outcome of the Security Evaluation where:

(a) the Target of Evaluation is the product of a parent company of the AISEF or another company in which the parent company has an interest;

(b) the Target of Evaluation is the product of a subsidiary company of the AISEF or another company or partnership in which the AISEF has an interest; or

(c) the AISEF has contributed to the development of the Target of Evaluation.

4.1.3 The AISEF warrants that at the date of signing this Agreement no conflict of interest, within the terms of paragraph 4.1.1, or any other conflict, exists and undertakes to immediately inform the Commonwealth if such a conflict arises.

Providing the conflict is known, or should have reasonably been known, to the AISEF or any AISEF employee. Where a previously unknown conflict is identified, steps will be taken to address the conflict to the satisfaction of the Australian Certifying Authority.

4.1.4 The AISEF shall not:

(a) provide consultancy services or advice to the Sponsor or the Supplier of the Target of Evaluation which would compromise the independence of the Security Evaluation;

(b) allow a person who has been involved in the development of the Target of Evaluation to be involved in a Security Evaluation of that Target of Evaluation; or

(c) otherwise compromise the independence of the Security Evaluation.

4.1.5 The AISEF shall not conduct a Security Evaluation unless the Target of Evaluation could reasonably be expected to satisfy the Evaluation Criteria at the ITSEC Level specified by the Sponsor.

4.1.6. The AISEF shall not collude with other companies granted AISEF status to set prices for the conduct of Security Evaluation, conduct Security Evaluations of products which have no reasonable prospect of satisfying the Evaluation Criteria or engage in any other unethical dealing.

Our view is that these conditions provide an adequate degree of separation between the operations of the AISEF and those of the parent company, even in circumstances where the parent company may offer products or services which are potentially in competition with a product that is under evaluation in their facility. The licence agreements provide for withdrawal of the AISEF's status and suspension or termination of the agreement in the event of a breach or failure to observe these obligations.

COST AND DURATION OF EVALUATIONS

Senator Lundy also noted claims by Optus that the evaluation process was too "extensive and expensive".

The first point to note is that the evaluation process that is used in the AISEP and equivalent schemes overseas is a recognized international standard (ISO 15408) that is rapidly becoming the benchmark for the evaluation of IT security products. A less extensive process of evaluation would be unlikely to achieve similar international recognition, and would most likely result in vendors having to put their products through a separate evaluation process for every country in which they wished to sell – the very problem which the Common Criteria was established to address.

With respect to the expense, the pre-evaluation and evaluation phases are by far the largest component of the cost; DSD charges a relatively minor fee to certify the results of the evaluation which is waived if the vendor/developer has a sponsorship letter from an Australian Government department or agency (which is generally the case). The cost of the evaluation and pre-evaluation services is dependent on the contract between the developer/vendor and the evaluation facility, which is a purely commercial transaction.

The cost and duration of an evaluation tend to be closely correlated, and the duration is extremely dependent on a wide range of factors which are beyond the capacity of any one participant to control. These factors include:

- the complexity of the product;
- the scope of the security functionality claimed by the developer/vendor;
- the level of assurance sought;
- how committed to (and experienced with) the process the vendor is; and
- the extent of problems identified in the course of the evaluation.

The effect of these factors is dramatic: for instance, a low assurance evaluation of a simple product with no cryptographic functionality may take a matter of months and cost tens of thousands of dollars, whilst a higher assurance evaluation of a more complex product (such as an operating system) could take years and cost millions of dollars. This makes the notion of an "average" duration fairly meaningless and makes direct comparisons between the AISEP and other schemes overseas difficult.

That being said, there are products currently in evaluation under the AISEP from vendors in the United States, United Kingdom, Canada and Germany (all of whom operate their own evaluation programs) and Korea. This suggests that these vendors, who have made a business decision to place their products into evaluation with the Australian scheme rather than their own (or another) national scheme, believe that – relatively speaking – the Australian scheme is performing on at least a comparable level.

Defence Signals Directorate
Information Security Group
Locked Bag 5076
KINGSTON ACT 2604

Ph: +61 2 6265-0197
Fax: +61 2 6265-0323

VIRTUAL PRIVATE NETWORKS

GENERAL

A Virtual Private Network (VPN) establishes secure network services over the range of network topologies including Local Area Networks, Wide Area Networks implemented on public and private infrastructures, and the Internet. While there is some complexity in determining an appropriate network model to be used and successfully implementing and managing it, there are significant benefits in being able to establish virtual secure private use of the public or private communications infrastructures that are already widely deployed and available, especially the Internet.

TREATMENT IN THE PSM AND ACSI 33

The Commonwealth Protective Security Manual (PSM), Part C, 7.140 – 7.141, acknowledges that there is higher risk within Australia when sending data over public networks such as the Internet, and provides guidance on protecting such data with Government Furnished or Government Approved Equipment. A solution for such protection could be the deployment of a VPN. Note that *The Commonwealth Protective Security Manual* does not strictly define private, public or virtual networks although it identifies the Internet as an example of a public network.

The Defence Signals Directorate's (DSD's) *Australian Communications-Electronic Security Instruction 33* (ACSI 33), Handbooks 1, 2 8 and 9, provide guidance on the establishment of a VPN. ACSI 33 provides guidance to agencies on:

- the level of encryption to be employed commensurate with the classification of the data to be protected;
- the use of DSD Evaluated Products; and
- the need to rigorously manage the network security services of:
  - authentication,
  - access control,
  - audit,
  - protection against malicious content, and
  - protection against leakage of date of higher classification to a lower classification network,

in the context of the security environment in which it is to be deployed.

SECURITY ISSUES

Security of communications via a VPN is enabled through the use of cryptography, usually deployed in the VPN network routers[1] or firewalls[2]. The predominant VPN protocol in use today is called Internet Protocol Security (IPSec). IPSec is an international standard protocol for interoperable network encryption and has gained acceptance among vendors of encryption products throughout the world. IPSec provides a framework within which encryption and authentication technologies can be employed in a standard way, allowing interoperability between IPSec products of different vendors. IPSec provides for the communications security features of data confidentiality, integrity, and non-repudiation.

IPSec uses public key cryptography to authenticate each encrypting device in the encrypted connection and symmetric keys to encrypt the data. IPSec defines the protocol for key management and allows devices to use a Certificate Authority and directory service to manage the keys. Together with the communications capacity offered by host networks such as the Internet, this greatly enhances the scalability of IPSec based solutions when compared to simpler network models and key management techniques. IPSec has been implemented in software and hardware in gateway network devices such as routers and firewalls, and in dedicated hardware devices.

In establishing a VPN over a Local Area Network, Wide Area Network or the Internet, only the network devices at each end of the communications path to be secured, are required to implement IPSec (see Diagram 1 below). The intermediate routers, of which there could be many, do not need to implement IPSec and simply pass the encrypted VPN data as they would any other data traversing the network. The specific sequence of intermediate routers used in the network may be unpredictable, and can change from one communication to the next. The specific path taken in the VPN is of no security relevance.

ADVANTAGES/DISADVANTAGES OF A VPN

The advantages offered by a VPN in comparison with a non-VPN network delivering comparable functionality over a geographically dispersed area are such that the non-VPN network would:

- tend to be more ‘point-to-point’ in nature, meaning that there would tend to be less redundancy in the available communications paths between locations. The loss of any one communications path is likely to have a more discernable, if not catastrophic impact on the ability to maintain communications;
- potentially be significantly more expensive to establish and maintain either through dedicated private cabling or communications lines leased from commercial telecommunications providers. This expense would be exacerbated with increasing geographical distance and communication points;
- be readily subject to security compromise unless comparable cryptographic services were implemented;
- be comparatively slow to deploy or modify; and
- not be as readily scaleable in expansion to new locations or in coping with increased data volumes in existing locations.

The disadvantages of a VPN are that:

- the IPSec protocol is complex and adds both a processing and data volume overhead;
- it requires specialist technical management; and

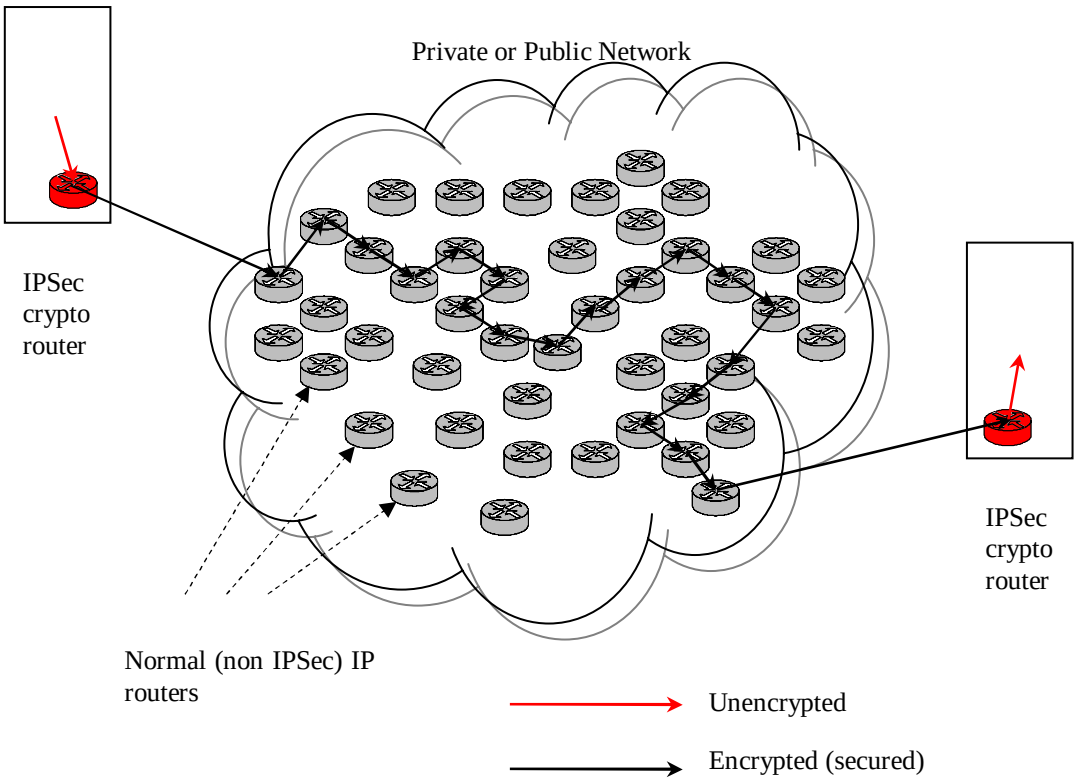
---

[1] A router is a device that determines the next network point to which communications data should be forwarded toward its destination. The router is connected to at least two network segments and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to.

[2] Firewalls can be an effective means of protecting networks and systems from external security threats while at the same time enabling access to external networks and systems via Wide Area Networks and the Internet.

- the risk of security breach by sending sensitive data to inappropriate destinations needs to be managed. With the security functions of a VPN being transparent to the end user, complacency about sending sensitive data to public destinations accessible on the network may develop unless mitigating controls are implemented.

Diagram 1 – A Typical Virtual Private Network



FEDLINK

Background

The National Office for the Information Economy (NOIE) created FedLink as an innovative and cost-effective solution for enabling secure communications between Government agencies. It is a VPN solution that provides secure and trusted communications across the Internet and is based on IPSec capable Cisco routers. These routers have been certified within the *Australasian Information Security Evaluation Program* (AISEP) to Evaluation Assurance Level (EAL) 4 - the level required to protect Commonwealth information classified up to and including PROTECTED. An agency connection to FedLink does not preclude their existing Internet connectivity. It does however mean that the security services offered by the VPN are only operative when communicating with another FedLink agency.

A number of security challenges arise as a consequence of using the Internet as the communications bearer for FedLink. Unlike a leased line where the two ends are known locations and the communications path generally known, information on the Internet may have travelled anywhere throughout the global network. Therefore, protocols used to pass data over the Internet must provide some guarantee of the sender's authenticity and provide confidence that the data will only be seen by the intended recipient, and was not modified in transit. The IPSec standard on which FedLink is based, was created to address security issues in a standard, vendor neutral way.

DSD Involvement

DSD has examined the FedLink architecture to be employed, the management arrangements to be implemented and agency connection requirements. The review was undertaken to ensure the appropriate protection of Commonwealth information while transiting the FedLink network. NOIE and DSD deemed that the FedLink solution was 'Fit for Purpose' prior to release by NOIE.

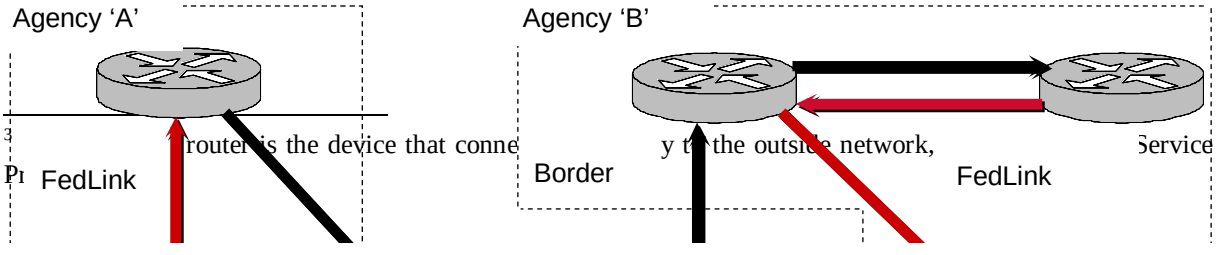
FedLink Architecture

FedLink is a system designed for secure data transmission at the inter-agency level. Its fundamental security claim is that between two FedLink agencies, data will be appropriately secured as it is transported over the Internet through the use of VPN technology. The FedLink VPN does not assure the data once the communication is decrypted on entry to the internal_network of the receiving agency. Separate appropriate security mechanisms must be implemented by the agency to protect Commonwealth data while resident within the agency internal network. It is important to remember that FedLink is an agency gateway to agency gateway, and not agency desktop to agency desktop solution. Similarly it does not provide security services for agency mobile users to establish secure remote access to agency networks.

FedLink is scaleable, and can potentially be used by all Commonwealth agencies and any other government (State or Local) or commercial entity with the need and approval to securely access or share classified Commonwealth data, classified up to and including PROTECTED.

Diagram 2 shows the standard FedLink configurations. These configurations allow for the appropriate handling of both FedLink and non-FedLink traffic. Agency A has the FedLink router in line with the agency's border router[3], meaning that all traffic must pass through the FedLink router. Agency B however has its border router interpret all traffic and passes the encrypted FedLink data to the FedLink router to be decrypted. In this diagram data is transmitted from Agency 'A' to Agency 'B'.

Diagram 2 – A Typical FedLink Configuration



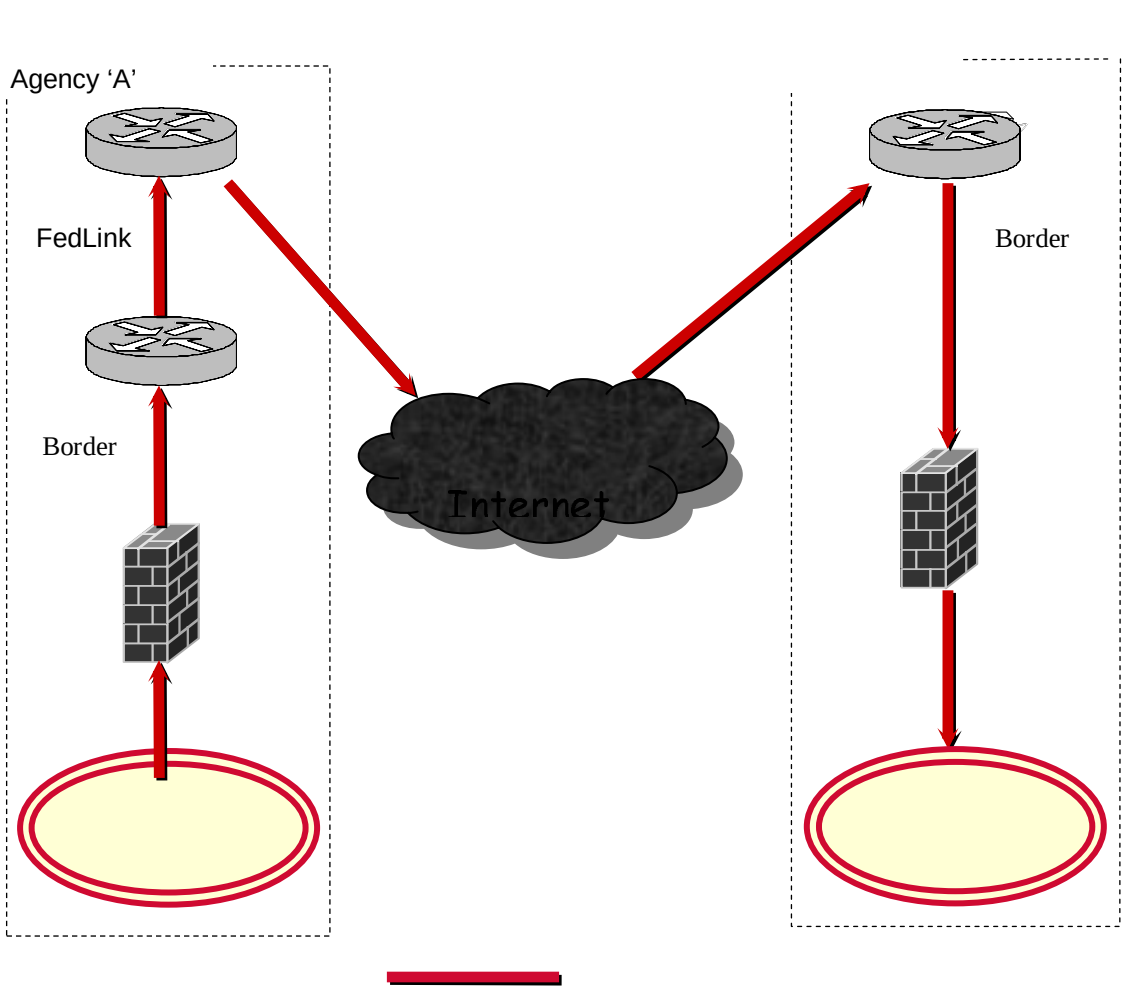
[3] router is the device that conne y t the outside network, Service

A FedLink router resides on the border of an agency's gateway examining the data as it is both received and sent. This router checks the data it is receiving and if that data has been sent by another FedLink agency, it decrypts that data. Any data from non-FedLink addresses is simply allowed to pass through the router into the secure gateway. When data sent by an agency passes through its FedLink router, the router checks the destination address of the data. If the address is another FedLink client, the data is encrypted and transmitted. If not destined for another FedLink registered agency the data is allowed to pass unencrypted through the router to the Internet.

As Diagram 2 illustrates, all traffic between the published IP addresses[4] of Agency A and Agency B was encrypted before it was transmitted. Diagram 3 shows that while Agency A is connected to FedLink, and all traffic passes through its FedLink router, data destined for Agency C must be transmitted unencrypted across the Internet as a consequence of Agency C not being connect to FedLink.

Diagram 3 – Normal Internet Traffic

[4] Internet Protocol (IP) addresses identify networks, and hosts or workstations within them. They form the basis of sender and receiver identification when communicating over the Internet.



As the FedLink IPSec routers are reliant on IP addresses in the implementation of the encryption policy, it is not necessary to encrypt all data to be sent through FedLink. FedLink agencies may decide, for example, to only encrypt email, in which case they would publish their email server IP address range to FedLink leaving all other traffic unaffected. In this way, the impact of the FedLink encryption and decryption processing overhead on an agency's bandwidth can be appropriately managed.

This list of FedLink registered IP addresses is an important piece of information to the successful operation of FedLink and is managed by the FedLink Support Facility (FSF). The FSF is provided and operated under contract on NOIE's behalf by 90East. Every two hours the list of IP addresses is securely updated to the routers allowing near real-time network management.

The FSF also supplies, maintains, and supports the FedLink routers, which are rented to agencies from the FSF. The policies and procedures associated with the operation of the FSF were assessed by DSD during the 'Fit for Purpose' review. DSD also conducts an annual review and makes the results available to NOIE.

Prior to connection to FedLink, an agency must prove its suitability to connect to the service. This means that the agency declares, by one of two methods, the ability to securely handle FedLink data. At an X-IN-CONFIDENCE level the agency can use either of two methods to prove this capability:

- Have the agency's gateway[5] environment certified either by DSD or an assessor registered by DSD[6]; or

[5] The DSD Gateway Certification process aims to provide a Commonwealth Agency, or a service provider to Commonwealth Agencies with an independent assessment that their gateway has been configured and managed to industry best practice and that appropriate safeguards are implemented and operating effectively.

[6] The Infosec – Registered Assessor Program (I-RAP), an initiative of DSD and administered by Standards Australia, endorses and registers information technology security assessors as competent to assess up to

- Supply a self-assessment review. A self-assessment review is completed by staff of the agency and then signed by the Chief Information Officer of the agency as meeting the requirements dictated by the self-assessment checklist (see attached).

Agencies connecting to FedLink at the PROTECTED level must send their data via a gateway certified either by DSD, or an assessor registered by DSD.

Other Possible Solutions

Some commercial providers, by using appropriate products on the *Evaluated Products List* to protect Commonwealth data, may be able to provide security services similar to FedLink that could be assessed by DSD. To date however, DSD has not been approached either by such service providers, or by Commonwealth agencies requesting DSD's formal review of these services.

PROTECTED level information security systems in accordance with Commonwealth information security standards and policies. The program specifically encompasses FedLink audits and connection assessments.