PIA for SSL Inspection implementation

Version: 1.0

Date: 1 August 2019

Owner: ICT Security

TRIM Number: D2019-80163

Background

The Security Improvement Program has a project to improve the perimeter cyber defences of Geoscience Australia's (GA's) ICT infrastructure. As part of the Perimeter Controls project, Secure Sockets Layer (SSL) Inspection will be implemented to mitigate the risk of cyber-attacks hiding within encrypted communications.

Personal information is transmitted across the network, in particular when used for personal purposes, for example, banking websites and online shopping. Due to the transmission of personal information, a threshold assessment is required to determine the types of privacy risks that may be realised and if a Privacy Impact Assessment (PIA) is required for SSL Inspection.

SSL Inspection will be implemented as an ICT security control recommended in the Information Security Manual (ISM). The malware scanning of personal information is an incidental outcome from this obligation.

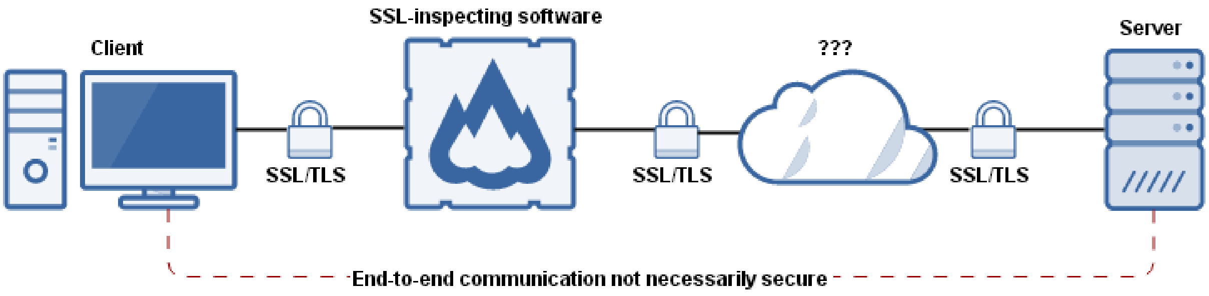
This assessment asks the question, is there any or a significant increase in privacy risks for users, as a result of the changes proposed?

References

- https://www.oaic.gov.au/privacy-law/
- https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments
- ICT Security Policy and Procedures (https://intranet.ga.gov.au/news/ict-security-policy-and-procedures)
- Privacy policy (http://www.ga.gov.au/privacy)
- Blue Coat URL categories: https://sitereview.bluecoat.com/#/category-descriptions
- *Security of Critical Infrastructure Act 2018* (Cth) (https://www.legislation.gov.au/Details/C2018A00029).

SSL Inspection Design

SSL Inspection will sit in the middle of the communications between a client machine and server. In GA's infrastructure, all web traffic from the corporate zone will pass through the SSL Inspection point. The SSL Inspection system establishes an encrypted connection to the user's workstation, and a second encrypted connection to the remote web server. These encrypted connections maintain the privacy of the user's communication with the remote server. At the SSL Inspection point, between the two encrypted connections, the Internet traffic passing through is scanned for malware, Trojans, and other cyber threats.



A key aspect of the design is that during normal usage the decryption and detection of malware and cyber threats is performed entirely by software – without human interaction. System logs (syslogs) will be systematically generated; syslogs only log events (metadata) and not the content passing through. Syslogs may assist in determining the source of any malware detected within Internet traffic, which can be achieved with the information in the header, e.g. URLs, date and time.

Privacy Risk Threshold

Determination if a system warrants an assessment of the impact on a user's privacy is via a threshold assessment. That is the standards, rights and obligations around the collection, use and disclosure of personal information.

The SSL Inspection system does not intrinsically collect or store information. In normal operation inspection of decrypted traffic is performed by software but in abnormal situations there is a risk that personal information, including possibly sensitive personal information, may be used or disclosed. Hence, the threshold test is exceeded and a PIA is required.

Privacy Impact Assessment

System based risks and mitigations

The following mitigations are in place for the risk that personal information may be inappropriately collected, stored, used or disclosed:

- The SSL Inspection system is entirely systematic and does not require a person to inspect the Internet traffic. All Internet traffic processed by the SSL Inspection system will be scanned by software (akin to a virus scan). A person with administrator access to the SSL Inspection system may be able to access personal information. Only authorised security personnel are permitted to access to the SSL Inspection and secure gateway systems.

These administrators have been granted the minimum level of privileged access required to perform necessary tasks, this is by design. The number of administrators with access is limited to the smallest number required. By capturing login events misuse will be tracked, thus deterring unauthorised access to the SSL Inspection system.

- The SSL system does not intrinsically collect or store personal information; only metadata logs will be kept. Only in the instance of a security incident (i.e. detection of malware or a virus in the encrypted traffic) will human intervention be required to review the metadata logs (syslogs). The syslogs have a short lifespan (30 days) before they are automatically deleted.
- The legal notice message at login has been revised to include “Internet usage will be monitored” to make users aware that all traffic, including potential personal information, may be monitored. Additional communication via the intranet and other means will be provided to alert employees of the changed behaviour before SSL inspection is implemented.
- Whilst legitimate business use does involve the transmission of personal information, e.g. email addresses, it is highly unlikely that the personal information provided in the course of business would lead to significant harm to any individual if misused. It is more likely that, in the unlikely case of misuse, significant harm may be caused to individuals using Geoscience Australia’s system for private use. Users have the opportunity to use their own systems if they are concerned.
- One of the risk mitigations in the scenario of a breach, is that any personal information that is compromised, cannot be systematically exploited. It would be a time consuming task to qualitatively find any value in the information. The risk mitigation for breaches is to invoke the Security Incident Management processes. An outcome of this process is the notification of a breach – and the dissemination of advice to change passwords.
- The SSL Inspection service will be sourced from a service provider with strong security practices and a current security certification. The proposed SSL Inspection and gateway security system is an Australian Signals Directorate Certified Gateway provided by Macquarie Telecom (MacTel). MacTel maintain this security accreditation which covers security vetting of staff and system access controls, in the same fashion as GA’s security vetting requirements and restricted access to systems. MacTel will be responsible for system security of the SSL Inspection and gateway security systems (the security controls) of these systems). GA will be responsible for security of syslogs provided as part of this system.
- All Internet traffic is categorised by Blue Coat Systems. A number of categories are exempt from SSL inspection; others are automatically blocked. For these two cases this project poses no increased risk to personal information. Only a limited number of categories will be subject to SSL inspection.

  Appendices A to C list the various categories and how they are treated.

  There is the potential for limited amounts of sensitive personal information to be assessed as some health related categories and union sites are included in the list of categories that are processed.

Risk Assessment

A risk assessment identifying the risks and controls of the proposed SSL Inspection in relation to the collection, storage, use or disclosure of personal information was undertaken (See **Appendix D**). This assessed that whilst the occurrence of the identified risks was possible, the consequences were minor, resulting in a risk rating within tolerance.

Conclusion

Some SSL traffic not currently inspected will be subject to inspection following the implementation of this system. This inspection in normal operation is entirely systematic; only metadata are retained and only for a short period. Exploitation of personal information would require administrator access and a significant degree of sophistication. Administrators are limited in number and appropriately vetted. Most common sites using encrypted communications are exempt from inspection; business use is unlikely to include sensitive personal information; and users wishing to use GA’s Internet for personal use can opt out.

As with all systems, there is a risk of exposure of information. However, in this case the residual risk to users’ privacy is low.

Recommendations

The following recommendations should be performed as part of the implementation phase of the project:

- Update relevant intranet pages with information on SSL inspection.
- Update ICT Procedures.
- Provide communications to all staff.

Appendix A

Website categories exempt from SSL Inspection

Internet traffic is categorised by Blue Coat Systems into a number of categories based upon an assessment of the site. These categories have been divided into three classes: those for which SSL inspection will not be performed; those where the traffic is blocked; and those where traffic is allowed but the site does not fall into a known safe site in which case SSL inspection will be performed.

The following list of website categories describes the use cases where SSL Inspection is exempt. For this use case, the increased privacy risk for users visiting these URLs is nil. Users will be able to nominate further services to be whitelisted.

URL Category	Control	Comments
Banking	Whitelist of sites exempt from SSL Inspection • Commonwealth Bank (www.commbank.com.au) • Westpac (www.westpac.com.au) • NAB (www.nab.com.au) • ANZ (www.anz.com.au) • St George (www.stgeorge.com.au) • ME Bank (www.mebank.com.au) • Macquarie Bank (www.macquarie.com.au) • Bendigo and Adelaide Bank (www.bendigoadelaide.com.au) • Bank of Queensland (www.boq.com.au) • Suncorp (www.suncorp.com.au) • Bankwest (www.bankwest.com.au) • HSBC (www.hsbc.com.au) • IMB (www.imb.com.au) • AMP (www.amp.com.au) • Credit Union Australia (https://www.cua.com.au/) • People's Choice Credit Union (https://www.peopleschoicecu.com.au/) • SERVICE ONE (https://www.serviceone.com.au/) • ING (www.ing.com.au)	• Users will be reminded of ICT Policy through the login legal notice.

Brokerage/Trading (e.g. share trading)	Whitelist of sites exempt from SSL Inspection • Commonwealth Securities (www.commsec.com.au) • Westpac Online Investing (onlineinvesting.westpac.com.au) • NABTrade (www.nabtrade.com.au) • ANZ Share Investing (www.anz.com.au) • CMC markets (www.cmcmarkets.com/en-au) • HSBC Online Share Trading (www.sharetrading.hsbc.com.au)	• Users will be reminded of ICT Policy through the login Legal Notice.
Auctions (e.g. eBay/PayPal)	Whitelist of sites exempt from SSL Inspection • Ebay (www.ebay.com.au) • Etsy (www.etsy.com.au) • GraysOnline (www.graysonline.com.au) • Amazon (www.amazon.com.au) • Paypal (www.paypal.com) • Allbids (www.allbids.com.au)	• Users will be reminded of ICT Policy through the login Legal Notice.
Shopping (e.g. Big W online shopping)	Exempt from inspection	
Radio/Audio Streams (e.g. YouTube)	Exempt from inspection	
Government	Whitelist of sites exempt from SSL Inspection • Australian government (*.gov.au) • New Zealand government (*.govt.nz) • US government (*.gov)	• Users will be reminded of ICT Policy through the login Legal Notice.

Appendix B

Website categories blocked by policy

The following list of website categories are those that are blocked by policy. For this use case, the increased privacy risk for users visiting these URLs is nil.

URL Category Name	Description
Adult/Mature Content	Sites that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These sites include very profane or vulgar content and sites that are not appropriate for children.
Child Pornography	Sites that include a visual depiction of a minor engaging in sexually explicit conduct.
Controlled Substances	Sites that discuss, encourage, promote, offer, sell, supply or otherwise advocate the use, cultivation, manufacture, or distribution of non-pharmaceutical drugs, intoxicating plants, solvents or chemicals, and their related paraphernalia. Typically these substances have no accepted medical use and a high potential for abuse. This category does not include alcohol, tobacco, or marijuana sites as these have a dedicated category.
Email	Sites offering Web-based email services, such as online email reading, and mailing list services.
Extreme	Sites that are extreme in nature and are not suitable for general consumption. Includes sites that revel and glorify in gore, human or animal suffering, scatological or other aberrant behaviours, perversities or debaucheries. It includes visual or written depictions deemed to be of an unusually horrific nature. These are salacious sites bereft of historical context, educational value or artistic merit created solely to debase, dehumanize or shock. Examples would include necrophilia, cannibalism, scat and amputee fetish sites.
Gambling	Sites where a user can place a bet or participate in a betting pool, participate in a lottery, or receive information, assistance, recommendations, or training in such activities. Does not include sites that sell gambling-related products/machines or sites for offline casinos and hotels, unless they meet one of the above requirements.

Games	Sites that support playing or downloading video games, computer games, or electronic games. Also includes sites that support or host online sweepstakes and giveaways.
Hacking	Sites that distribute, promote or provide tools or other information intended to help gain unauthorised or illegal access to computers, computer networks, or computerised communication and control systems. Also includes sites with instructions for creating or distributing malware or information on performing cyber attacks.
Intimate Apparel/Swimsuit	Sites that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. Does not include sites selling undergarments as a subsection of other products offered.
Malicious Outbound Data/Botnets	Sites to which botnets or other malware (as defined in the Malicious Sources category) send data or from which they receive command-and-control instructions. Includes sites that contain serious privacy issues, such as "phone home" sites to which software can connect and send user information. Usually does not include sites that can be categorised as Malicious Sources.
Malicious Sources/Malnets	Sites that host or distribute malware or whose purpose for existence is as part of a malicious network (malnet) or the malware ecosystem. Malware is defined as software that takes control of a computer, modifies computer settings, or collects or reports personal information without the permission of the end user. It also includes software that misrepresents itself by tricking users to download or install it or to enter personal information. This includes sites or software that perform drive-by downloads; browser hijackers; dialers; any program that modifies your browser homepage, bookmarks, or security settings; and keyloggers. It also includes any software that bundles malware (as defined above) as part of its offering. Information collected or reported is "personal" if it contains uniquely identifying data, such as email addresses, name, social security number, IP address, etc. A site is not classified as malware if the user is reasonably notified that the software will perform these actions (e.g., it alerts that it will send personal information, be installed, or that it will log keystrokes).
Marijuana	Sites that discuss, encourage, promote, offer, sell, supply or otherwise advocate the use, cultivation, manufacture or distribution of marijuana and its myriad aliases, whether for recreational or medicinal purposes. Includes sites with content regarding marijuana-related paraphernalia.

Nudity	Sites containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include sites containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist sites that contain pictures of nude individuals.
Peer-to-Peer (P2P)	Sites that distribute software to facilitate the direct exchange of files between users. P2P includes software that enables file search and sharing across a network without dependence on a central server.
Personals/Dating	Sites that promote interpersonal relationships.
Personal Sites	Sites consisting primarily of user-generated content that serves as a vehicle for self-promotion on which a variety of personal experiences or interests are shared. These sites do not represent businesses, institutions or governmental entities although they may mention or be sponsored by such bodies. Content on these sites tends to be dynamic in nature. Content topic and tone may vary from benign to extreme or vacillate between the two as determined by the author. Reader comments may also contain mixed content.
Phishing	Sites that are designed to appear as a legitimate bank or retailer with the intent to fraudulently capture sensitive data (i.e. credit card numbers, pin numbers).
Placeholders	Sites that are under construction, parked domains, search-bait or otherwise generally having no useful value.
Pornography	Sites that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
Potentially Unwanted Software	Sites that are not malicious sources but that host software with undesirable behaviour or cause undesirable browser behaviour such as such as intrusive adware, adware servers used exclusively by intrusive adware, and browser hijackers.
Proxy Avoidance	Sites that provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server. This category includes any service which will allow a person to bypass the Blue Coat filtering system, such as anonymous surfing services.

Religion	Sites that promote and provide information on traditional, organised religious belief, practice and observance and directly-related subjects such as religious catechism or dogma and places of religious worship or observance (e.g., churches, synagogues, temples, etc.). This category does not include sites about non-traditional spiritual and non-religious belief systems (Alternative Spirituality/Belief).
Remote Access Tools	Sites that primarily focus on providing information about and/or methods that enable authorised access to and use of a desktop computer or private network remotely.
Scam/Questionable/Illegal	Sites that advocate or give advice on performing acts that are illegal or of questionable legality such as service theft, evading law enforcement, fraud, burglary techniques, and plagiarism. Also includes sites that promote scams such as work-from-home, pay-to-surf, and Ponzi schemes and sites that provide or sell legally questionable educational materials such as term papers.
Sex Education	Sites that provide information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, tips for better sex, and sexual enhancement products.
Sexual Expression	Sites that provide information about, promote, or cater to sexual expression and sexual identity in all its forms including the full range of sexual practices, interests, orientations, and fetishes. Does not include sex education which is categorised in the Sex Education category or content that is sexually gratuitous in nature, which is categorised in the Pornography or Extreme categories.
Spam	Sites that are part of the spam ecosystem, including sites linked in unsolicited bulk electronic messages and sites used to generate or propagate such messages.
Suspicious	Sites considered to have suspicious content and/or intent that poses an elevated security or privacy risk. This categorization is determined by analysis of web reputation factors. Also includes sites that are part of the Web and email spam ecosystem. If a site is determined to be clearly malicious or benign, it will be placed in a different category.
Uncategorised	Sites that are not currently rated or that cannot be rated into any other category.

Violence/Hate/Racism	Sites that depict extreme physical harm to people, animals or property, or that advocate or provide instructions on how to cause such harm. Also includes sites that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics. Includes content that glorifies self-mutilation or suicide.
Weapons	Sites that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. Does not include information on BB guns, paintball guns, black powder rifles, target shooting, or bows and arrows unless the site also meets one of the above requirements. Also does not include sites that promote collecting weapons, or groups that either support or oppose weapons use.
Web Ads/Analytics	Sites that provide online advertisements, banners, or the means to identify and market to existing or potential customers based on their browsing or online purchasing habits including but not limited to Web analytics sites such as visitor tracking and ranking sites. Includes social plugins and analytics that allow site visitors to share, vote for, or signal their appreciation of a site or its content (e.g. Facebook "Like" or Google "+1" plugins).

Appendix C

Website categories to be processed

The following lists all remaining categories. These will be subject to SSL inspection.

URL Category Name	Description
Abortion	Sites which provide information or arguments in favour of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion.
Alcohol	Sites that discuss, encourage, promote, offer, sell, supply, or otherwise advocate the use or creation of alcoholic beverages, including but not limited to beer, wine, and hard liquors. It does not include sites that sell alcohol as a subset of other products such as restaurants or grocery stores.
Alternative Spirituality/Belief	Sites that promote and provide information on a wide range of non-traditional and/or non-religious spiritual, existential, experiential, and philosophical belief systems. Includes sites related to atheism, agnosticism, and mysticism; sites related to quasi-religious, philosophical or spiritual belief systems and practices that do not include formally established religious meetings, places of worship, organizational structure, or dogma; and sites that endorse or offer information about affecting or influencing real events through supernatural or magical means. Also includes sites that discuss or deal with paranormal or unexplained events. This category does not include sites centered around traditional, organised religious belief, practice, and observance (Religion).
Art/Culture	Sites that nurture and promote cultural understanding of fine art including but not limited to sculpture, paintings and other visual art forms, literature, music, dance, ballet, and performance art and the venues or foundations that support, foster or house them such as museums, galleries, symphonies and the like. Sites that provide a learning environment or cultural awareness outside of the strictures of formalised education such as museums and planetariums are included under this heading.

Business/Economy	Sites devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include sites that perform services that are defined in another category (such as Information Technology companies, or companies that sell travel services). Does not include shopping sites.
Charitable Organizations	Sites that foster volunteerism for charitable causes. Also encompasses non-profit associations that cultivate philanthropic or relief efforts. Does not include organizations that attempt to influence legislation as a significant portion of their activities or organizations that campaign for, contribute to or affiliate with political organizations or candidates.
Chat (IM)/SMS	Sites that provide chat, text messaging (SMS) or instant messaging capabilities or client downloads.
Content Servers	Servers that provide commercial hosting for a variety of content such as images and media files. These servers are typically used in conjunction with other web servers to optimize content retrieval speeds.
E-Card/Invitations	Sites that facilitate the sending of electronic greeting cards, invitations or similar electronic messages typically used to mark an event or special occasion.
Education	Sites that offer education information, distance learning, or trade school information or programs. Includes sites that are sponsored by schools, educational facilities, faculty, or alumni groups.
Entertainment	Sites that provide information about or promote popular culture including but not limited to film, film critiques and discussions, film trailers, box office, television, home entertainment, music, comics, graphic novels, literary news, and reviews. This category also includes entertainment-oriented periodicals, interviews, fan clubs, celebrity gossip, and podcasts; and music and film charts.
File Storage/Sharing	Sites and services that provide online file or note storage, file sharing, synchronization of files between devices and/or network-based data backup and restoration. These services may provide the means to upload, download, paste, organize, post and share documents, files, computer code, text, non-copyright-restricted videos, music and other electronically formatted information in virtual data storage. Does not include Office/Business Applications or Media Sharing.

Financial Services	Sites that provide or advertise banking services, lending services, insurance services, financial information, or advice on a variety of fiscal topics including loans. Does not include sites that offer market information, brokerage or trading services, which are categorised in the Brokerage/Trading category.
For Kids	Sites designed specifically for children. This category is used in conjunction with other categories - it is not a stand-alone category.
Health	Sites that provide advice and information on general health such as fitness and well-being, personal health, medical services, over-the-counter and prescription medications, health effects of both legal and illegal drug use, alternative and complementary therapies, medical information about ailments, dentistry, optometry, and general psychiatry. Also includes self-help and support organizations dedicated to a disease or health condition.
Humour/Jokes	Sites that primarily focus on comedy, jokes, fun, etc. May include sites containing jokes of adult or mature nature. Sites containing humorous Adult/Mature content also have an Adult/Mature category rating.
Informational	Sites that provide content that is informational in nature and does not provide a way to directly act upon the information (e.g., a site that provides lottery results, but does not sell lottery tickets). This category is always used in conjunction with another category appropriate to the subject matter (e.g., gambling).
Internet Connected Devices	Sites that allow management and monitoring of or network access to physical devices connected to the Internet. Such devices include but are not limited to network infrastructure such as routers and switches, network-enabled industrial equipment, security cameras, home automation equipment, and other Web-enabled devices. Also includes security camera feeds, which are dually categorised as TV/Video Streams.
Internet Telephony	Sites that facilitate Internet telephony or provide Internet telephony services such as voice over IP (VOIP).
Job Search/Careers	Sites that provide assistance in finding employment, and tools for locating prospective employers.
Media Sharing	Sites that allow sharing of media (e.g., photo sharing) and have a low risk of including objectionable content such as adult or pornographic material.

Military	Sites that promote or provide information on military branches or armed services.
Mixed Content/Potentially Adult	Sites with generally non-offensive content but that also have potentially objectionable content such as adult or pornographic material that is not organised so that it can be classified separately. Sites that explicitly exclude offensive, adult, and pornographic content are not included in this category.
News/Media	Sites that primarily report information or comments on current events or contemporary issues of the day. Also includes news radio stations and news magazines. Does not include sites that can be rated in other categories.
Newsgroups/Forums	Sites that primarily offer access to newsgroups, messaging or bulletin board systems, or group blogs where participants can post comments, hold discussions, or seek opinions or expertise on a variety of topics.
Non-Viewable/Infrastructure	Servers that provide Internet infrastructure services and information used by applications but not necessarily viewable by web browsers. Includes security services such as security patch downloads, anti-virus database updates, content filtering systems, shared authentication services, and certificate management services such as OCSP and CRL services. Traffic and content in this category is neither malicious nor objectionable in nature and may be required for applications or network traffic to function properly.
Nudity	Sites containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include sites containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist sites that contain pictures of nude individuals.
Office/Business Applications	Sites with interactive, Web-based office, productivity, collaboration, and business applications including business enablement services. Excludes email, chat/IM, or other sites that have a specific content category.
Online Meetings	Sites that facilitate online meetings or provide online meeting, conferencing or training services.
Political/Social Advocacy	Sites sponsored by groups or individuals that provide information on political parties, special interest groups, organizations, factions or individuals that promote change or reform in public policy, public opinion, social practice, social justice, or related economic activities. Includes sites that advance political or social agendas, lobby for political or social change, facilitate civic

	engagement, and advocate personal or collective action in its multiple forms including but not limited to petitioning, boycotts, and demonstrations.
Real Estate	Sites that provide information on renting, buying, or selling real estate or properties. Also includes vacation property rentals such as time-shares and vacation condos.
Reference	Sites containing personal, professional, or educational reference, including online dictionaries, maps, censuses, almanacs, library catalogues, genealogy-related sites and scientific information.
Religion	Sites that promote and provide information on traditional, organised religious belief, practice and observance and directly-related subjects such as religious catechism or dogma and places of religious worship or observance (e.g., churches, synagogues, temples, etc.). This category does not include sites about non-traditional spiritual and non-religious belief systems (Alternative Spirituality/Belief).
Remote Access Tools	Sites that primarily focus on providing information about and/or methods that enable authorised access to and use of a desktop computer or private network remotely.
Restaurants/Dining/Food	Sites that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes.
Search Engines/Portals	Sites that support searching the Internet, indices, and directories.
Social Networking	Sites that enable people to connect with others to form an online community. Typically members describe themselves in personal Web page profiles and form interactive networks, linking them with other members based on common interests or acquaintances. Instant messaging, file sharing and Web logs (blogs) are common features of Social Networking sites. These sites may contain offensive material in the community-created content. This category may be used in conjunction with another category for more narrowly-focused social networking sites, such as professional networking sites or social networking sections of Personals/Dating sites.
Society/Daily Living	Sites providing information on matters of daily life. This includes but is not limited to pet care, home improvement, fashion/beauty tips, hobbies and other tasks that comprise everyday life. It does not include sites relating to entertainment, sports, jobs, personal pages or other topics which already have a specific category.

Software Downloads	Sites wholly dedicated to the download of software for any type of computer or computing device whether for payment or at no charge. Does not include sites or pages that offer a software download as a subset of their overall content.
Sports/Recreation	Sites that promote or provide information about spectator sports or recreational activities. It does not include sites dedicated to hobbies such as gardening, collecting, board games, scrapbooking, quilting, etc.
Technology/Internet	Sites that sponsor or provide information, news, reviews, opinions and coverage of computing, computing devices and technology, consumer electronics, and general technology. Also includes sites of technology-related organizations and companies.
Tobacco	Sites that discuss, encourage, promote, offer, sell, supply, or otherwise advocate the use or creation of tobacco or tobacco-related products including but not limited to traditional or electronic cigarettes, pipes, cigars, chewing tobacco, hookahs, or nicotine delivery systems. Does not include sites that sell tobacco as a subset of other products such as grocery stores.
Translation	Sites that allow translation of text (words, phrases, web pages, between various languages) or that can be used to identify a language.
Travel	Sites that promote or provide opportunity for travel planning, including finding and making travel reservations, sharing of travel experiences (pro or con) vehicle rentals, descriptions of travel destinations, or promotions for hotels/casinos or other travel related accommodations. Mass transit information including but not limited to posting of schedules/fares or any other public transportation-related data are also included in this category.
Vehicles	Sites that provide information on or promote vehicles, boats, or aircraft, including sites that support online purchase of vehicles or parts.
Web Hosting	Sites of organisations that provide top-level domain pages, as well as web communities, blog hosting sites, and other hosting services.

Appendix D

Risk Assessment - Privacy Impact Assessment for SSL Inspection

Risk Assessment

Objective	Risk (the effect on the objective)	Source/s (events or non-events that could cause the risk to eventuate)	Controls	Risk with controls					Risk with treatments
				Likelihood	Consequence/s	Consequence category	Risk rating with controls	Within tolerance?	Possible treatment/s
To assess and ensure that personal information is collected, stored, used or disclosed in accordance with the Privacy Act 1988 -	SSL Inspection may result in the inappropriate collection, storage, use or disclosure of personal information.	• Accidental disclosure of personal information. • Intentional disclosure or misuse of personal information.	• The SSL Inspection system does not require a person to inspect the Internet traffic. • Only authorised security personnel are permitted to access to the SSL Inspection and secure gateway systems. • The SSL system does not intrinsically collect or store personal information. Only metadata logs will be kept. • A revised Legal Notice message at login, to include "Internet usage" will be monitored to make users aware that all traffic, including potential personal information, may be monitored. Users have the opportunity to use their own systems if they are concerned. • Source the SSL Inspection service from a service provider with strong security practices and a current security certification.	Possible	Minor	Reputation	Low	Yes	No further treatments required, but may implemented after cost/benefit analysis
				Possible	Insignificant	Compliance	Very low	Yes	
				Possible	Minor	Security	Low	Yes	