Security Survey

1. **SSL Certificate**
   Secure Sockets Layer (SSL) is a global standard security technology developed by Netscape in 1994. SSL creates an encrypted link between a web server and a web browser to ensure that all data transmitted remains private and secure. Millions of consumers recognize the "golden padlock" which appears in their browser to indicate they are viewing a secure web page. Our SSL Certificate is managed by Comodo (www.comodo.com)

2. **Retention Policy**
   Information is retained in the system for a minimum of two years. Some types of information are required to be retained for five to seven years to comply with state and federal laws. Access to information is based on User permission levels that are specified by the client and Verify-Ed. Any email addresses that are associated with the specific search subject or system user and will never be shared with any other entity or used for any purpose other than that which is specifically authorized by the person to whom it belongs.

3. **Confidentiality Measures**

   Security Policy

   The Security Policy operates at three levels: 1) Physical security; 2) Operational security; and, 3) Systems security. It is recognized that highly sensitive information is handled through our systems as well as by its personnel on a daily basis. Thus, the controls and procedures that have been implemented help to assure the security of that information as well as the physical systems underlying its operations. Each of the three levels is intertwined with the others to assure a comprehensive approach to the overall security.

   Physical Security

   Physical security begins with the physical premise of our associated offices as well as the Network Center hosting the network equipment. The building is monitored 24/7 and has restricted cardkey access during non-business hours.

   Once inside the main building doors, the office is protected by a separate cardkey system with intrusion monitoring and web camera monitoring. Finally, the Network Center has restricted cardkey access that requires a separate permission level than the main office area. Within the office area, all sensitive files are maintained within locked file storage. Office computers do not store sensitive material on local hard drives to prevent possible unauthorized access. Any paper item slated for disposal is shredded prior to disposal.

   Operational Security

   The operational security begins with proper training for personnel regarding the handling, processing, storage and disposal of confidential search information. Security awareness is reflected in the handling of all client information and search submissions and results. Each client has separate electronic and physical file structures to ensure separation of information. Only individuals directly involved in providing client services have system access. Physical files are maintained in locked file storage and obsolete paper files are destroyed via shredding prior to disposal. Electronic files are stored within the system database in an encrypted structure to avoid possible unauthorized access and viewing. The files are stored indefinitely for subsequent retrieval and compliance purposes by clients.

   Facsimile communications are handled in a secure location with restricted access. All received facsimile communications are initially received on a facsimile server to ensure

privacy. Authorized personnel retrieve the facsimile transmissions from the server for processing.

Workstations operate Microsoft Windows XP that allows for security control of the local unit. All workstations are locked upon a preset inactivity time-out to ensure the prevention of unauthorized viewing of search requests and results.

Systems Security

Systems security is integrated into the software at the base level. Authorization categories are established for all users with permission levels set based on individual access criteria. The system Username and Password protection is supplemented with control logs and transaction logs that record activity within the system.

All search transactions, both submissions and retrievals, occur via a secure Internet connection that is protected by Secure Socket Layer 128-bit encryption for privacy. E-mail communications can also be secured with encrypted transmission and digital signatures to ensure tamper-resistant communications. Our system does not use email as a primary communication tool. Rather, email notifications are sent to provide a secure link back into the system that is fully protected by the SSL encryption.

All system network servers are located within a secure physical environment with both biometric and attendant monitoring. The actual servers further protected with login security for administrative access. Backup/disaster recovery files are maintained on separate Network Attached Storage devices that are mirrored to another facility daily for redundancy and disaster recovery purposes. All sites are monitored for intrusion detection and fire safety.

The network system is configured with separate Web servers and database servers to heighten security and avoid possible unwanted intrusions by unauthorized people. In addition, the Web and database servers are protected by a Netscreen firewall and intrusion detection server. All system access and performance are monitored on a real-time basis.

Other security features of our system include automatic masking of social security numbers on any printout materials to minimize the potential for identity theft. The system has automatic time-out protection to terminate access in the event of inactivity at any client workstation (i.e., someone steps away from their desk and forgets to logout).

4. Employee Safeguards

All employees are subject to comprehensive background checks and provided job training specific to their responsibilities. Training includes the proper handling, processing, storage and disposal of confidential search information. Our security awareness is reflected in the handling of all client information and search submissions and results. Each client has separate electronic and physical file structures to ensure separation of information. Only individuals directly involved in providing client services have system access. Physical files are maintained in locked file storage and obsolete paper files are destroyed via shredding prior to disposal.

5. Hardware and Software Requirements

Internet access and a computer with a Web browser (i.e., Internet Explorer, Mozilla Firefox) that is CSS2 compliant. There are no software installation requirements.

6. Email Requirements

No attachments are sent via email. All communication takes place via a secure 128-bit encrypted Internet connection.

All email communications are approximately 10kb in size.