Security

Physical and Information Security
The Bureau maintains model security policy and procedures for its core business functions–the provision of media capture, document processing, conversion, telecommunications, translation and other related products and tasks.

WebsiteThis website collects no user specific data. Communications options are available that allow you to send e-mail directly to Bureau employees. Information within e-mails that you send to Bureau employees-including your e-mail address-will not be sold, transferred or otherwise distributed to other commercial or non-commercial entities.

Security PolicyThe Bureau takes strong precautions regarding the security of customer data. Internal user education and the Bureau's centralized data center is at the forefront of the Bureau’s information security policy. Education includes mandatory yearly privacy training for all levels of staff, signed employment agreements, signed ethics and privacy agreements and background investigations of employees. For non customer data such as internet access, automated filters and servers monitor incoming data, check for, flag and eliminate virtually all SPAM e-mail, malware (i.e., adware, spyware and viruses) and potentially dangerous online activity.

To highlight the primary security systems and policies in-place at the Bureau, security is handled at three (3) primary levels, each with several sub-items.

1. Physical Security
   a. Site and building
   b. Hard copy and physical media
   c. Supporting infrastructure
2. Information Technology Security
   a. Servers and storage
   b. Workstations
   c. Internal and external networks
   d. Authentication and access control
   e. Customer communications
3. Personnel Security
   a. Training
   b. Background
   c. Agreements, contracts and formal policy
   d. Audit and oversight

Physical SecurityFor physical security, the Bureau maintains heavy duty three (3) and four (4) tumbler deadbolt locks with 18 inch stainless steel anti-penetration plates on all entrances to its headquarters and Arizona offices. The downtown Chicago and Milwaukee offices have security staff on-premises with logged entry. The Bureau headquarters in Burr Ridge has an additional double entryway with foyer and a monitored alarm system with door, window, IR and glass breakage sensors along with 24/7 monitoring and logging.

Hard Copy SecuritySince 2003, all administrators and their assistants were furnished with heavy duty cross-cut shredders for strict adherence to the thoughest mandates and policy of our customers. This includes the destruction of any hard copy, notes, faxes, magnetic media and optical media with protected customer information. Sensitive hard copy material is secured in a fire-rated vault at the end of each business day.

Media SecurityCustomer data including captured media and completed documents are stored in a centrally located document management cluster in the Bureau's class III data center, not on staff workstations. This centralized functionality was originally engineered for the Bureau’s document processing infrastructure for our government, law enforcement, legal and medical clients. But, this technology is now used for all clients. This processing methodology pays numerous dividends that ensure customer data is treated with confidentiality while still having the highest levels of availability and full audit capability.

Remote User Security

Remote employees utilize high-speed certificate-based SSL VPN (i.e., authenticated and encrypted) network connections for streamed media transfer and document management access. No media is stored on an employee system and the resulting documents and logs are stored centrally as well.Customer Communcation

Work transmitted back to customers securely using the most appropriate method based on customer needs and capability. Options include the use of an automatic callback modem-to-modem connection with encryption, site-to-site VPN tunnel (e.g., for direct access to your socket servers, network shares and other servers), on demand VPN tunnel, certificate-based (PKI) encrypted e-mail, encrypted archive, FTPS and more. In addition, compound methods of security are often used such as PKI encrypted e-mail delivery of application encrypted documents.Infrastructure Integrity and Security

Security is enhanced by the stability afforded by the Bureau's infrastructure including our class III data center. Bureau servers are all rack-mounted in segmented racks, powered by split phase power distribution, backed up with enormous commercial-scale battery back up, powered by an automatic and a full-facility natural gas generator during extended power outages. Auxilliary, temperature-controlled condenser cooling along with a frost-proof cold air intake operate 24/7/365.

All computer systems (including remote systems on-site at customer locations) at the Bureau is protected by an uninterruptable power supply (i.e., UPS or battery backup unit). All employees use uninterruptable power with all computer systems.Data Security

Data stored on Bureau servers is protected by three (3) layers of authentication, one (1) layer of high-level encryption and two (2) layers of network segmentation. Should systems and servers be physically compromised, internal and customer data is safe. In addition, nightly rotating backups protect data from accidental, intentional and failure-based loss.Audit and Logging

All systems which process customer data have meticulous logging capability at every step. Steps including data and media capture, speech recognition, editing, transcription, quality assurance, data export, remote review, data transfer, interfacing, backup and archiving all create detailed audit trails. "Lost" data and reports are a thing of the past.