U. S. Department of Justice
Information Technology Strategic Plan

Appendix B

The Prospects for Technology Insertion

White Paper

Appendix B
The Prospects for Technology Insertion White Paper*

It would not be practical for DOJ's information infrastructure to be on the leading edge for every information technology vector. The reasons DOJ cannot be state of the art across all technology vectors include:

- It is unaffordable. Following technology too closely means discarding systems while they are still functional and economic, undertaking repeated installation costs, and putting users and administrators through continual retraining.

- It carries risks. The first few versions of new technologies are often flawed, not "industrial strength" and may have security weaknesses that are not initially apparent.

- It presents potential barriers to interoperability beyond DOJ to the extent that other groups (e.g., working on a given case) may not have such leading-edge capabilities.

- It is not always necessary. DOJ has many systems that work quite well today and which provide a stable baseline for coordinated improvements. Technology upgrade or replacement should be predicated on a business justification.

- It requires a workforce inconsistent with the compensation limitations imposed on DOJ.

Consequently, DOJ needs to evaluate various technologies broadly and determine which ones appear to have the largest impact on DOJ and its mission. Technology areas that offer potential breakthroughs for DOJ effectiveness and efficiency will warrant more attention and risk taking than those that do not. Figure 1 is a heuristic spectrum of five technology strategy choices that range from being a technology driver to being a follower or, in the case of special requirements, a laggard.

- DOJ would be a *driver* of a technology if its requirements were unique, singular, or clearly leading-edge enough to pay for their development. For the Department of Defense (DoD), many technologies (largely those without civilian application) fall into this category. DOJ has far fewer such requirements; forensics is the most obvious example of a unique technology requirement.

- DOJ would be a technology *leade*r if it had sufficient need for a technology that it were willing to (1) pay the high cost of acquiring such a technology when it was introduced and (2) suffer through the inevitable difficulties in using and securing such technologies. For some technologies, the DOJ and its components may need to drive its advancement through establishing standards and funding development either directly or indirectly (e.g., biometric scanning). For others, the DOJ will not assume this leadership role but may decide to be out in front with an advanced but commercially available technology (e.g., data mining tools).

- DOJ would be a technology *early adopter* if it had a strong requirement for the technology and could make use of it early. An early adopter would deploy a technology once it is commercially

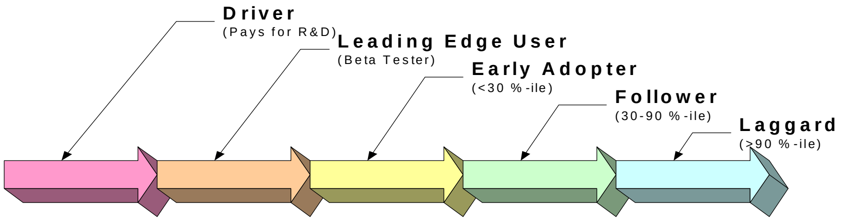
* This White Paper is based on unpublished material prepared by the Rand Corporation for the Department of Justice.

available and proven but not widely installed. Generally, the business benefits would justify an earlier adoption and offset the higher costs and risks of early adoption versus deferring until the technology matures.

- DOJ would be a technology *follower* if its requirement for the technology were no stronger than that of comparable organizations. Waiting until other organizations have deployed the technology usually reduces the time, cost and risks involved and allows one to take advantage of others' lessons learned.

- DOJ would be a deliberate technology *laggard* if it had special requirements that were either met only by previous but not current generations of technology (e.g., applications available only for older operating systems) or because it needed extensive maturity in technologies to prove their rock-hard stability.

Figure 1
When Should Technology be Adopted?



Six technology areas are discussed below. The discussion is in two parts: the first part is a quick tutorial of the potentials and maturity of the technology; the second is an examination of ways DOJ might use the technology. Because DOJ is composed of components and subcomponents, a general assessment of DOJ's stance on a technology (e.g., DOJ should be an early adapter of this and a follower of that) does mean that such assessments necessarily apply to all components equally.

Sensors and Biometrics

Sensors and biometrics acquire a large component of all information collected from the ambient environment (in the case of sensors) or from individuals (in the case of biometrics). Both involve the conversion of physical facts into information (in some cases without further interpretation). As with any sensing technology, the percentage of all information so acquired that, later, becomes useful for law enforcement is random and small.

State of the Art and Current Trends

Although the U.S. Army has made tremendous strides in the development of unmanned ground sensors, the relevance of its work to DOJ requirements is tangential inasmuch as many of DoD's parameters (e.g., well-funded applications to support short-term usage in territory without uncontested access) do not apply to DOJ. Tactical unmanned aerial vehicles under development for the Army and the U.S. Marine Corps may have applicability to DOJ once they become sufficiently reliable and under human control to share the nation's air spaces. Perhaps the most useful trends in sensors has been in the consumer sector. One aspect has been the proliferation and sharply falling costs of devices such as digital cameras, night-vision optics, infrared detectors (as intrusion detectors), and high-gain microphones. Another has been the rapid decline in the cost of so-called "smart tags," global positioning system (GPS) devices, and low-power transmission gear (controlling bovine herds electronically is becoming increasingly feasible). Combining cheap electronics and low-cost networking promises to improve the efficiency of wide-area surveillance networks.

How Can Technology be Used?

Sensors come in stand-alone forms (e.g., bomb-sniffing machines) and networked mode; the latter is relevant to DOJ's information strategy, notably for border control. INS runs a fully-sensored network, the Integrated Surveillance Information System (ISIS), that monitors the southwestern border of the United States to detect movements that may indicate illegal immigration or narcotics smuggling. DOJ should be a technology *early adopter* in the area of wide-area sensors and their integration into fully developed situational awareness suites. In this regard, it should stay abreast of the DoD as it develops similar technology for military purposes so that it can step in to adapt such sensors to the exigencies of its target physical and legal environment. The overall strategy for such a network is to push in the direction of increased acuity and coverage, as well as faster response-times and lower maintenance and installation costs.

Biometrics is another rapidly developing field in which DoD, again, has taken the lead (notably through the Defense Advanced Research projects Agency's (DARPA) human-ID-at-a-distance program). DOJ should be a technology *driver* in the application of biometrics to forensics, notably in (1) pushing the state of the art in making effective use of continually smaller and less-than-perfect biometric samples, and (2) making faster determinations of matches between collected and archived biometrics. DOJ should be a technology *leader* in the application of identifying people at a distance and in the exploitation of other biometric techniques such as signatures, voiceprints, and associated metrics.

DOJ should pursue an aggressive strategy of acquiring fingerprint reader devices. Modular upgrades to the JABS program may provide the correct vehicle for such acquisition for the USMS, BOP, and DEA.

Appendix B
The Prospects for Technology Insertion White Paper

Case Support Tools

Investigators, prosecutors, and litigators must all cope with vast heterogeneous collections of information that must be accessible in near real time and may yield further results if they can be correlated (much as data mining promises for sufficiently structured data). Tools that would assist in this process include those that support:

- Case management,
- Automatic voice and handwriting recognition,
- Automatic language translation,
- Assisted content-tagging,
- Data visualization,
- Data mining, and
- Knowledge management.

State of the Art and Current Trends

Legal cases are multi-faceted and complex. They require tailored software to assist in its management. Case management systems entail the management of documents, which can include: securing documents; handling and maintaining different versions of them; searching through and retrieving them based on words or phrases. These systems can also assist in time and relationship management with calendaring, contacts files, "ticklers" for reminders of upcoming deadlines and events, and so on. To serve the specialized needs of large law firms, vendors[1] have developed a variety of products.

Case management software typically includes one or more of the following:

- *Relationship management (link analysis)*: can track an indefinite number of contacts, each with an unlimited number of addresses, phone numbers, and related cases; integrate contact information with telephone system (e.g., "click to dial"); integrate contact information with office automation address books; and use online "notes" attached to contact information.

- *Document management*: can support document scanning; full-text indexing of word processing documents (including the ability to search for words by phonics, word stems, or synonyms); document check-in and check-out facilities (so only one person on a case can modify a document at one time); control over read-only, modification, and check-in/check-out rights for specific documents.

[1] A representative set includes: Prolaw Software (www.prolaw.com), LegalEdge Software (www.legaledge.com), Legal Files Software Inc. (www.legalfiles.com), Gavel & Gown Software Inc. (www.amicusattorney.com), Abacus Data Systems Inc. (abacuslaw.com), Software Technology Inc. (ww.stilegal.com), and ADC Legal Systems Inc. (www.adclegal.com.). A broader index can be found at www.netesmartinc.com/software.htm). This listing in no way implies endorsement of such products by the DOJ.

- *Rules-based calendaring*: can manage deadlines for a particular case, event and meeting arrangements, docket event tracking, reminders, and integrate itself with office automation calendars.

- *Records management*: can track the complete history of every file; integrate with bar codes for document tracking; and access scanned files.

- *Conflicts searching*: can check all other cases that case-related parties have been associated with.

- *Time tracking, billing and accounting*: can track time spent on various tasks, integrated with billing and accounting systems if needed.

- *Report generation*: can design custom reports through "drag and drop" of fields.

- *Web accessibility*: can support access to case information via a World Wide Web page ("portal") with access control, for remote (home, hotel, office) access to common case files.

As a general rule such software can be integrated with word processing packages, a variety of operating systems, E-mail clients, palmtop clients, spreadsheet-scanning systems and they support the Legal Electronic Data Exchange Standard (LEDES) developed by PriceWaterhouseCoopers. Although the capabilities mentioned above are important functions of relevance to law enforcement, they come with substantial requirements for initial implementation, subsequent maintenance, and integration with other software systems.

The improvement of *voice and handwriting recognition products* has been and is likely to remain gradual; a breakthrough in either is unlikely. Major software houses (e.g., Microsoft) are eager to incorporate such technologies into their offerings once they reach a certain level of reliability; the growing ubiquity of palmtops and smart cellular telephones is likely to push progress forward somewhat faster. Within a five to ten year period such products may overcome the current obstacles so that the cost and hassle of entering information by voice or hand and then manually correcting the output of such products drops below the cost of entering such information by keyboard.

Automatic language translation is also characterized by slow steady progress, but without the handheld market to drive it forward. Given the amount of computing power and data stores required for automatic language translation, it may be better provided as a subscription service hosted on heavyweight servers and accessed via a Web-client than as standalone products. In the United States, this market is being driven in large part by the needs of DoD and the intelligence community.

*Automated tagging tool*s are used to annotate free-form text and other such data so that it can be machine-processed for search and retrieval, as well as publishing. The advent and widespread acceptance of XML (eXtensible Markup Language) has created a grammar and method for tagging. The corresponding development of standard tag sets has proceeded slowly . The prospects are good, however, that within a few years, there will be a standard tag set for the litigation and investigation community.

Data visualization tools convert data into graphical artifacts in order to enhance human understanding of their contents. As with speech and handwriting recognition, progress is slow but steady; what works for one may not work as well as for another; and tool standardization is not really needed for such tools to work together (data may have to be in standard format for such tools to work, however).

Data mining tools comprise another set of techniques to help uncover insights from large volumes of structured data. Six techniques are commonly used: neural net analysis (capable of "learning" from given examples to make plausible predictions), decision tree analysis (which uses binary dichotomy methods), clustering algorithms (to discover like features within data sets), affinity analysis (to generate if-then rules), case-base reasoning (class-matching algorithms; but losing favor as a technique), and genetic algorithms (that gradually improve prediction fitness; not yet ready for general use). Two general rules should be noted. First, data mining tools assist analysis but users have to know what they are looking for first. Second, such tools have to be specific both to their data sets and to their inquiries; a tool that shows, say, that disposable diapers and beer are often purchased in the same shopping trip is not the same as one that can build patterns of association among criminals.

Knowledge management promises organizations that it can collectively know the sum total of what its employees individually know. It comes in two flavors: one helps to organize information (e.g., find me a report on the involvement of parking enforcement in the drug trade), the other organizes people (e.g., find me a person(s) who knows about this subject, experience, etc.). Sometimes a knowledge management system is as simple as a culture (and a network) that lets people pose questions to the community as a whole and expect a cogent response. As a rule of thumb, in any field with less than 200 professionals, people will know of each other well enough to abjure automated systems for acquiring such information.

How Can Technology be Used?

As a general rule, the seven technologies of this section are rapidly evolving tools rather than mature, integrated product suites. As such, while there may be a long-term goal to equip DOJ with the latest case support tools, given the fluid nature of the environment at this time, this is not an area in which DOJ should make elaborate long-term plans. The likely (and preferred) scenario calls for purchasing such tools, as compelling needs and opportunities are defined by groups within DOJ. Many of the first purchases will be pilots or experiments and some experiments will not pan out. Others will work; people will be satisfied and/or more effective with the experience and recommend others do the same. At some point, the successfully applied tools will become more mature and will warrant establishing standards and broader rollout.

With regard to case management tools, DOJ would be a technology follower because their needs are unlikely to differ significantly from major multi-office, multi-national law firms, in this area. In light of the expected difficulties of owning such complex software, DOJ strategy should put a heavy emphasis on site visits to large distributed users of different systems under consideration prior to adopting such tools.

With regard to voice and handwriting recognition tools, DOJ would be a technology follower. What is important is not that each tool interoperate with each other but that each work well (e.g., produce reliable digitized text from verbal or written word). The acquisition of such tools by DOJ would be very useful (especially for the litigating and investigating components) in completing its digitization program, and thus the progress of such tools should be actively monitored.

DOJ would be a follower in automatic language translation, either letting the intelligence community take the lead, or looking for a Web-based service and signing up as a client.

DOJ should be an early adopter of automated content tagging tools once such tools are commercially viable. Tag set standardization for the legal community (prefatory to the use of automatic tagging tools) merits a strong DOJ participation. Getting people to tag documents (in whatever tag set), however, is far more difficult -- akin to asking software developers to document their code or getting intelligence analysts to classify each paragraph they write. But like software, annotation at some point has to take place if case materials are to be truly usable by people at remove from the case itself; good tools will hasten that day.

With regard to data visualization tools, DOJ would be a technology follower, keeping abreast of developments.

DOJ should be an early adapter of data mining tools. As noted, the benefits of having an integrated database of persons assume some sort of data mining capability. Although there are desktop data mining tools, the assumption is that a serious data mining application is likely to sit on its own heavyweight server. Here, the recommended strategy is to experiment robustly with alternative models, pay attention to their specific requirements for data, and, if any appear promising, acquire them as one would a major program.

DOJ should be a technology follower in knowledge management software. These tools can be useful for larger communities; within them it has to be installed widely if it is to be at all useful (and, if it is installed, should cover the broader law enforcement community and not just DOJ's portion); it also has to be carefully designed and implemented. It should stay abreast of technological developments but hold off on implementing its own systems until they are proven useful elsewhere and until the potential benefits to DOJ can be documented.

Collaboration Tools

Collaboration tools are used to enhance interactions among people and permit the creation of virtual teams from people who work for different components or in disparate locations. Enabling tools include video teleconferencing, whiteboarding, groupware, and the ability to commonly reference material. Implicit in many collaboration tools is that material can be organized in a logical and intuitive manner. The ideal here is for every virtual team member to log into a collective effort and be presented, not only with access to other team members, but also a structured case collection that can be visualized and subject to formatted queries.

State of the Art and Current Trends

Many DOJ activities, notably case management, require collaboration, both within groups of individuals within one location or office, and between geographically distributed groups. The state of the art falls under three categories: supporting infrastructure, collaborative application tools, and content repository.

Infrastructure: Collaboration requires a network infrastructure that provides many-place many-time access to secure information and communication (any-time any-place access is better, but not always realistic in some situations.) The following discussion assumes team members are collaborating on a "case" (but has a broader relevance) that stretches, project-like, with a beginning, middle and end spanning months or years, and with variable team membership (both from case to case and within a case over time) composed of individuals who may, themselves, be associated with multiple cases. These individuals may be DOJ employees or consultants, affiliates of other government agencies (federal, state, local) or international organizations (e.g., Interpol, other countries' DOJ or INS equivalents). What matters is the ability to create new groups of communication partners with access to at least some parts of the secure network infrastructure on a case-by-case basis, and to add (or delete) individuals quickly and easily.

The network infrastructure must be accessible to case team members from their offices and their homes as well as on the road (in many locations); it should be possible to send/receive still images at least in most situations. The state of the "infrastructure" art is maturing rapidly, with a number of international companies (e.g., InfoNet with its "DialXPress" service) offering thousands of "gateways" (local telephone numbers) into a protected network based either on separate, leased lines, or facilities to tunnel through the Internet with encrypted messages.

Collaborative applications and tools: These comprise an extensible repertoire of end-user software embedded in the network infrastructure and/or its clients. These applications and tools should provide support for work group collaboration among case team members. For convenience, such software can be grouped into three subsets[2] with somewhat fuzzy boundaries; they reflect increasingly specific and active roles for collaborative applications and tools.

Special collaboration tools facilitate timely and effective interaction among case team members. Examples include items mentioned above under "case management": address books; interface to secure fax, phone, and printers; special fields in documents to allow explicit threading; automated filing and retrieval; deadline markers; and so on. Cooperation support tools

[2] [following Malone, Olson and others in the computer-supported cooperative work research community]

include specialized facilities to support particular types of multi-person cooperative interchanges, such as:

- Real-time in-person or distributed conferencing, smart whiteboard-like applications, shareable and manipulable group artifacts (e.g., models, flow charts, if-then scenarios),

- Asynchronous distributed technologies that provide at least similar capabilities (e.g., asynchronous conferencing with posting alerts), and

- Decision support tools

Cooperation support tools are emerging from the domain of "peer-to-peer" (P2P) networking. For instance, the Groove Networks system (www.groove.com), which provides a common workplace for distributed participants, provisions for shared document folders, email, chat, shared program "tools" *et al*, security and encryption, the capability to configure multiple workspaces and restrict access to invited participants. This system is P2P in that the content of these workspaces is distributed to participants' computers, and not centralized in any one location. This architecture also provides considerable resilience and robustness, with no single point of failure. In such tools, the software, itself, takes on an active role in managing cooperative activities. Examples include intelligent agents playing rule-based roles in planning, exploring, fact-finding, decision-making, and technologies that provide routine or event-triggered roles in moving the work flow (e.g., enterprise resource planning (ERP)-like systems, some document management systems).

DARPA is addressing the problem of complex, distributed information systems built from heterogeneous components. One example is BBN’s Assured Assembly Infrastructure (AAI) Toolkit (see aai.bbn.com) whose aspirations includes permitting the dynamic composition of systems based on real-time feedback of system state, on expressed requirements for system services, and on expressed dependencies between system components. Dynamic composition of systems will benefit long-lived distributed systems by providing adaptability in terms of satisfying evolving requirements under evolving operating conditions.

Related DAPRA work includes the Habitats system, involving user “agent” programs that negotiate with the system and other agents within it to provide access to services and facilities that users require. These programs also rely on “object-oriented” software technologies, in which software modules contain both data and the operations to be performed on those data.

Content repositories: Multiple databases will undoubtedly be involved in collaboration. Users need common interfaces and search/browse tools to give them the perception of dealing with one large but well differentiated repository of information with relevance across multiple cases. Quite likely these databases would serve other non-case purposes as well (e.g., report generation, organizational learning, knowledge management, and data mining). Examples of types of contents may include directory information, quantitative or other structured data (e.g., arrest records, motor vehicle records, visa request rejections, and so on), text reports (background information, memoranda), and images (photos, fingerprints). For content repositories to be useful they must be initially accurate and be maintained/updated on a known and appropriate schedule. It should be possible to search them readily, accessing case-related information and storing it in appropriately useful chunks (perhaps in some sort of case-defined temporary store). Finally, there should be easy-to-invoke links between different types of data potentially residing in different databases (e.g., it would be desirable to be able easily to link quantitative data and a related background report about illegal alien activity at defined borders).

How Can Technology be Used?

Many of the individual components of a collaboration suite, such a video teleconferencing and whiteboarding, are fairly mature. Some DOJ components (e.g., EOUSA) are actively investing in such technologies for their own purposes. Other aspects of collaboration, such as the ability to annotate interactions, or to have background materials come up without being summoned are still in the laboratory.

By and large, however, collaboration tools have not been widely deployed, in large part because they do not feel “right.” They have yet to capture the social and organizational dynamics of the way people work – with their panoply of social cues, side-comments, and accidental encounters -- in a natural way (robust networking helps but only partway). There remains considerable (and often justified) skepticism that the results of using collaboration tools are worth the bother of learning how to use them effectively. Part of the problem is one of expectations. It would be nice to create a virtual environment in which new entrants to, say, a case or investigation, feel as comfortable as those who have been on it for a long time do. But simply throwing the case materials at someone and hoping this brings them up to speed is hardly adequate; there is a considerable body of tacit knowledge built into a case which is hard to capture easily. Another part of the problem is one of standards; bridging the gaps between still-proprietary systems is difficult.

Nevertheless, given the benefits of information sharing, and the multi-jurisdictional nature of many of DOJ’s toughest challenges (e.g., counter-terrorism, counter-narcotics) the benefits of being able to do virtual teaming are very high. The DOJ strategy, therefore, should be to launch some collaboration pilots. Once one or two pilots pass the test of real usefulness, the experiment should be extended to other interested entities within DOJ. If and when these tools become mature and ingrained in how people operate, their wide-scale rollout within DOJ litigation and investigation components and beyond them to other law enforcement entities could represent a significant process improvement breakthrough.

DOJ should be an early adopter in content repositories. Many DOJ components work with the same groups—criminals, aliens, etc. so managing relevant content and providing secure access could enable substantial operational improvements and business process transformation.

Appendix B
The Prospects for Technology Insertion White Paper

Remote Access

To help spur overall communications competition based on wireless technology, the U.S. and other governments have begun efforts to reallocate spectrum. The DOJ, along with other U.S. Government agencies, has been forced to revamp its wireless communications infrastructure under the mandate that it cut its need for spectrum by 75% within the next five to ten years.

State of the Art and Current Trends

Remote access to data and voice communications networks – whether via wireless or wire-line service – has changed tremendously in the last five years. Technology now makes it possible for DOJ employees to access DOJ voice and data networks from their homes, desktops, colleagues' offices, and the field. This opportunity will only grow over the next five to ten years. Network access entails a broad swath of technologies from radio frequency communications based on licensed and unlicensed spectrum, to copper wires and coaxial cabling of existing service providers, and fiber-optic facilities deployed by incumbents and startups alike. These technologies support both voice networks and a broad array of data networks based on transport protocols such as Ethernet, Frame Relay, ATM, and IP – all available in both public and private forms.

The Telecommunications Act of 1996 and other forms of deregulation has spurred the deployment of new access technologies, and new network operators to offer them. This market is in the midst of a major restructuring, which has yielded a complex telecommunications landscape with glut (largely in the backbone) and shortage (largely in the last mile), vendors with unpredictable business futures, and a cornucopia of choices. Nevertheless, the cell phone is on its way to becoming a ubiquitous fixture in urban areas. That plus the fact that computers and Internet are features of most American households has blurred the line between home and work. Households, in turn, are beginning to switch from dial-up to broadband access; at least 10 million use either high-speed cable or DSL to get to the Internet. In business, wireless access technologies combine with notebook computers to enable workers to fetch e-mail, intranets, and corporate databases from desktop, conference room, or off-site alike. Airports and coffee shops are beginning to experiment with providing Internet access. Broad access coupled with VPN (virtual private network) technology are making obsolete the very notion of a desktop as the only possible workplace – particularly for those whose gather, analyze and use information. Meanwhile computers are becoming general-purpose communications devices thanks to instant messaging service, voice-over-IP capabilities, and stream media. Pagers and cell phones are undergoing this transition in reverse; they become capable of exchanging text, web pages, pictures, and even video.

No single, unifying access technology is likely to emerge as universal as twisted pair copper wiring was for telephony. If nothing else, differences in geography and history will see to that. Similarly, no single access standard is likely to become ubiquitous. Nevertheless, at least three standards – HTTP (for Web access), TCP/IP (for the Internet), and Ethernet (for local-area connections) – are so entrenched that betting against them in any context is likely to be foolish.[3] IP,

[3] Other aspects of access standards and technologies are difficult to forecast with any confidence. Consider wireless data

especially, is likely to dominate as the underlying protocol of choice for universal data transfer. The standard, itself, is on the verge of shifting from the IPv4 implementation to a newer IPv6 implementation. Although it is unclear when the best time to switch from one to the other will be, it probably will not be within the next few years.

Services such as voice, e-mail, and instant messaging are expected to converge based on a common IP transport layer. Technologies, standards and services such as VoIP, H.323 videoconferencing, SIP (Simple Internet Protocol), and instant messaging may well become the basis for a substantial worldwide market to carry long-distance voice services over data networks. If trends continue, business data and voice communications are expected to merge into a single service offering. Video may eventually join this convergence.

Public policy will place increasing amounts of spectrum in the hands of commercial network operators. Communications is becoming a commodity, dominated by economies of scale. Access technologies, and networks suitable for use by DOJ will largely remain in private hands in the next five years. There will be competition among private network operators; however, that competition may be limited to where the reach of large access networks overlaps such as between competing cellular franchises or between cable TV operators and incumbent DSL providers.

How Can Technology be Used?

DOJ's path to enhanced remote access can be discussed in terms of three steps:

First, all DOJ employees would be able to log into their workspaces from any DOJ office. For example, an investigator working with a prosecutor on a criminal case would be able to access investigative information resources from the DOJ network at the prosecutor's office to help the prosecutor in preparing the case. At a minimum this requires that all DOJ component networks be sufficiently and simultaneously interconnected and well secured – a departure from the current security model that relies on electronically disconnecting networks from the rest of the world. Thus, the upgrading of OA tools would be coupled by security infrastructures that employ alternative methodologies to enhance security.

Second, such capability would be extended to other U.S. Government worksites (e.g., courts) through common remote access technologies (e.g., a secure 802.11b/802.11a infrastructure).

Third, such capability would be extended to any location in the field. The goal is to enable all DOJ employees away from the office (or even away from a table) to log into their workspace, retrieve and send important messages, and, better yet, participate as a full-fledged member of a virtual or physical team.

access. Although Europe has a single standard (whose deployment awaits sufficient capital), the U.S. cellular market is based on several standards, each with its own strategy for evolving to broadband data access. While all of this is debated among the carriers and governments, the 802.11b (and 11a) standards are being used to implement 10Mb/s+ access networks in locations like Starbuck's and airports. There are hints that cellular carriers are considering deploying similar technology [ref].

Appendix B
The Prospects for Technology Insertion White Paper

The mandate to reduce spectrum use, coupled with the burgeoning development of wireless options for data access offers DOJ an excellent opportunity to rethink its wireless strategy. DOJ must replace its current voice-only wireless infrastructure with something that accommodates data – but is nevertheless compatible with DOJ's stringent security requirements and the geographical distribution of its workforce . Similarly, DOJ must examine where it can best utilize commercial wireless voice and data services to meet its needs. This may, for instance, entail investments in token-based authentication and VPN software for notebook computers and handheld devices that assure authentication, authorization, and privacy and integrity of data regardless of the public network used to access DOJ networks.

DOJ should also recognize that these wireless networks are a competitor to the traditional networks for voice services, as well as data services. While cellular phones, like any other technology, is unlikely to be a universal strategy for DOJ, it may be a suitable targeted alternative to PSTN-based services to assure that DOJ is getting the best prices for services such as local and long-distance voice and voice messaging.[4]

Telecommunications trends point to a future DOJ network design utilizing multiple commercial service providers for access (and backbone) networks.[5] No single carrier will be able to provide universal service for DOJ's needs, and resilience and recovery concerns dictate the use of multiple carriers. Furthermore, even the largest of these carriers may face financial difficulties in the future. Thus, DOJ must develop network architectures that are based on heterogeneous access technologies, and that minimize the substitution of one carrier for another.

Access technology is closely coupled to security concerns. Wireless techniques, notably 802.11b and its putative successor 802.11a, have unacceptably bad security, whether used in a DOJ facility, in an employee's home, or in public (e.g., at an airport). Fixed point-to-point wireless (e.g., free space optics, MMDS, LMDS, and VSAT systems) also has a role in DOJ in providing access to DOJ backbone networks at remote offices. DOJ's use of these technologies must either await better security or the development of virtual private network (VPN) tools that encompass all DOJ LAN nodes using wireless access. These same security tools (e.g., token-based authentication, link- or end-to-end encryption, virtual private networks, etc.) can also be used over public networks to provide access to DOJ networks. Examples include employees using their Internet Service Providers to access DOJ networks from home or hotels, and using public networks to implement communications links between DOJ facilities.

[4] Cellular billing plans have virtually eliminated the distinction between local and long-distance prices. Cellular service is by definition mobile and eliminates much of the cost and delay associated with carrier or PBX managed wire-line services (e.g., Centrex).

[5] GovNet may emerge a component of DOJ's access and backbone networks. It is currently envisioned as an "air-gapped" network assuring secured, reliable government communications. It is likely that a GovNet would only be applied to "essential" DOJ operations, and not to all of DOJ's network needs. Furthermore, it seems unlikely that an extensive GovNet would be facilities based. It would likely be completely or partially built using encrypted links over public networks providing access and backbone transport.

Appendix B
The Prospects for Technology Insertion White Paper

There are currently two primary devices used for remote access: laptops and palmtops. A growing percentage of worksites will have wireless connectivity to the Internet and, as they do, DOJ equipment should be prepared to take advantage of that fact (e.g., via PCMCIA cards in laptops). For those sites without 802.11b or similar access, the next best option is direct wireless access through a wide-area provider. Yet, as noted below, the bandwidth that would more than satisfy a handheld, may not satisfy a laptop with its greater capacity to display and store information.

The quest for a wireless solution for handhelds raises four issues: adequate bandwidth, adequate coverage, security, and emergency services. As noted, current services, on average, can deliver 10,000 bits per second. This is adequate for exchanging E-mail and black-and-white images (e.g., on the RIM Blackberry) but inadequate for full-fledged data access, the easy use of high-end palmtops (e.g., Compaq's iPaq), or the transfer of even gray-scale images. Within five years, it is likely (but by no means certain) that access speeds (at least in metropolitan areas) will reach 64,000 to 384,000 bits per second. At 64,000 bits per second, a high-end handheld screen (240 x 320 bits) can be filled with a compressed image in one to three seconds (depending on color depth, the degree of detail, and overhead). 64,000 bps is therefore quite adequate, and 384,000 would be excellent. Down the road, it will also be important that these handheld units be able to *transmit* at adequate transmission rates. Many handhelds support cameras. There is no technical reason that a suitably modified handheld cannot acquire slap fingerprints as well (since a full-fledged fingerprint file is roughly a megabyte, transmitting one would take roughly two minutes over a 64,000 bps connection). As all these services come to be offered, DOJ could prototype their use with field agents of a component that do not have stringent security requirements.

In the meantime, DOJ (perhaps in conjunction with other U.S. Government agencies) would look hard for a secure solution for wireless data transfer. A key requirement is that third parties that capture a handheld device not be able to log into the Department's databases or network services without some further authentication mechanism (e.g., a PIN number or biometric).

Three issues are yet to be resolved before DOJ can move off its current voice-only self-managed wireless system (not to be confused with point-to-point wireless systems such as walkie-talkies): voice service, coverage (especially in the southwestern border areas), and emergency capabilities. Getting voice, of course, is the *sine qua non* of any decision to abandon the wireless system; yet, with proper client-side modifications, any system that can transmit data can also transmit voice-over-IP (compressed voice streams can easily fit within 10,000 bps service). Coverage can be met in one of two ways: by special arrangements with a service provider (e.g., via contract or incentive-rate purchased commitments), or by space-based systems.

Emergencies, for their part, come in two types: unexpected service interruptions or unexpected usage patterns (e.g., the congestion of cell phone service in Manhattan after the Twin Towers were hit). Space-based systems have the characteristics that their individual cells are very large; thus even a local emergency that congests local cell service may register only a blip within the larger space-based cells. Nevertheless, both terrestrial and space-based communications offerings are in flux and it is by no means certain which ones, or even if any, are viable business propositions.

The DOJ strategy for replacing its current generation of handhelds should put a premium on retaining today's service for now and wait to see how the market shakes out. In the likely event that high-bandwidth data services become available, then the active and intelligent exploitation of such services is the preferred path. Again, depending on market conditions (e.g., the population of low-earth orbit space-based communications), a backup and low-density strategy of using low-earth orbiting space-based communications has a good deal to recommend it.

Finally, the overwhelming role of commercial communications infrastructures within DOJ's overall communications mix, combined with the shortfalls revealed in the wake of the Twin Towers bombing together focus attention to the rules administered by NCS that govern emergency access to such networks. DOJ will help prepare future initiatives to define the responsibilities of carriers to provide government emergency communications services in future emergencies. Realization of these capabilities would then be factored into planning the architecture of DOJ access and backbone networks.

Wide-area Networking

Irrespective of whatever else DOJ invests in, it needs a viable, low-cost, wide-area networking solution to connect its offices and headquarters. The current Justice Consolidated Network (FBI aside) runs roughly 500 megabits per second into an ATM backbone. When, not if, the rest of DOJ adopts patterns of network demand that the FBI will (once Trilogy is complete), it can expect a tenfold demand increase – and that is not even counting the expected year-to-year growth in the installation of bandwidth-hungry applications (e.g., to support collaboration, or wireless connectivity). Wide-area networking solutions that are affordable at 500 megabits per second do not scale to affordability with one or two orders of magnitude more demand.

It is also important that DOJ's WAN infrastructure maximize flexibility so that the system as a whole is robust against failure (e.g., losing one component does not lead to a global breakdown). The WAN's architecture should also pose no barriers to information sharing and collaboration across components.

State of the Art and Current Trends

The forces that drive access network technology also affect wide-area networking. De-regulation has created competition for long-distance voice services, and data services. The late 1990s saw new fiber-based backbone data networks and sharp declines for both data and voice services. The restructuring of the telecommunications industry highlighted an apparent excess of long-haul bandwidth and put companies, both new and old, in financial difficulties.

Wide-area networking includes not only long haul circuits, but also metropolitan area networks (MANs), which remain an important component in DOJ's backbone network. Their existence provides a major source of competition for connecting sites in the same city, and a potential way to aggregate traffic for a DOJ long-haul backbone.

DOJ's networks are IP based. These IP networks must be implemented with one or more link technologies providing transport between DOJ locations. In addition to leased lines, there are extensive national and metropolitan networks that offer ATM and Frame Relay services, available from multiple operators, which can be used to construct DOJ's IP networks. These ATM and Frame Relay networks are typically public networks that switch the traffic from multiple customers over common links and switches in their backbones. VSAT technology is also a candidate, but requires a careful thought about how to tradeoff the limited bandwidth and long latencies of a VSAT against the advantages of a non-terrestrial path between routers.

Although ATM and Frame Relay have extensive legacy networks likely to stay lit for years to come, they are facing increasing competition from fiber optic technologies (e.g., IP over SONET, IP over physical fiber, Ethernet over MANs) in linking IP routers. The slow improvement rate of line cards for ATM and Frame Relay switches contrasts with much faster improvements in line cards that support SONET or fiber directly. The advent of dense wave division multiplexing may accelerate improvements in the costs of transporting bits. True, both ATM and Frame Relay (over an ATM backbone) support prioritization of traffic, and can be somewhat simpler to use. Yet, PVCs can be used to allocate increments of bandwidth between routers in IP networks with only minimal consideration of the underlying physical connections. UBR, VBR and CBR choices offer different ways to prioritize the traffic placed on different PVCs sharing the same physical facilities. In an IP over fiber network, a more complex performance analysis is required because the transport mechanism does nothing to manage the bandwidth of the physical circuit. Mechanisms, such as MPLS, are being introduced to help manage and provision bandwidth in these "pure" IP networks, as well as prioritize traffic based on QoS criteria.

ATM, Frame Relay, SONET, Ethernet, and fiber are all technologies suited for building a private IP network. VPN technology, which permits traffic to be encrypted and tunneled through the Internet, can permit the Internet itself to be an alternative backbone facility for DOJ.

How Can Technology be Used?

DOJs networks are IP and will remain so. In the next five years, IPv4 is likely to remain the dominant version of IP. If IPv6 emerges in that time frame, it will probably do so with wireless networks used for mobile access. If it does, DOJ will need an IT strategy for achieving interoperability of its mobile, wireless data networks and its backbones.

Ultimately, WAN strategies are issues of bits-per-dollar, once security and redundancy requirements are satisfied. In a world in which relative prices shift drastically from one year to the next, flexibility is essential in garnering the lowest price. Conversely, locking into one technology to the exclusion of others is generally unwise. While national ATM and Frame Relay (over ATM) are likely to continue in operation in the next several years, they are not likely to offer the most cost effective solution, given technology trends.

Appendix B
The Prospects for Technology Insertion White Paper

The current contenders for WAN service are Frame Relay (over ATM), ATM, and IP networks – the last of which might be based on a carrier's shared IP network including the Internet itself. There is little question that economics, and the relative availability of networking equipment, are increasingly favoring native IP transport. The actual prices charged for such services will vary by location and circumstance and there are real limits to how often one should change technologies based on momentary price advantages. At any one point in time DOJ's WAN infrastructure may use a mix of Ethernet, native IP and ATM. Nevertheless, the trends are clear. Early indications are that a public IP solution is already five to ten times less expensive per bandwidth than an ATM solution. All DOJ IP networks should be designed in a way that anticipates the use of multiple technologies and that minimizes the impact of substituting one carrier for another.

The lowest-cost solution, putting DOJ entirely on the Internet, however, exposes DOJ operations to the vagaries of the Internet. The obvious threat is from viruses/worms and hackers. This threat, however, comes from any exposure to the Internet, such as comes from the DOJ gateway in Rockville. The less obvious threat, and one that ATM systems are not nearly as prone to, is from a denial-of-service attack. One type is a failure in the Internet's routing and addressing infrastructures; another type is attempts to flood the connections used by specific users (e.g., the February 2000 distributed denial-of-service attack aimed at various E-commerce web sites). It should be noted that a denial-of-service attack that saturates links between routers could affect ATM systems indirectly, if ATM (UBR) is being used to implement a saturated link.

IP solutions, as such, come in two flavors: private and public. A *private* IP solution for DOJ would be designed so that internal connections would be safeguarded even if connections to the rest of the world were imperiled; in effect, there were be an ISP-maintained firewall between DOJ and the universe. There are two ways to do this: in hardware (e.g., air-gapping) or through software. Given the near-impossibility of a hardware solution, exactly how "private" such a service would be can only be judged by evaluating the ISP and carriers used to build the DOJ IP network.[6] A *public* IP solution means connecting DOJ up to the Internet one node at a time. This requires replacing DOJ's one firewall (to ward off hackers and viruses/worms) with hundreds or thousands of firewalls. Unless and until the various threats to the Internet have somehow mitigated themselves, this is a viable solution for DOJ only if: (1) adequate backup were present, and (2) multiple firewalls could be configured and administered as though they were one.

Recovery and reconstitution of the DOJ WAN also need attention. Point specific faults (e.g., equipment failures, fiber cuts, etc.) are common and their effects should be anticipated and mitigated in an IP network design. These are more likely than region-specific failures (e.g., from major terrorist incidents, weather-related problems), which are more likely than nationwide-failures (e.g., from a wholesale Internet attack, or nuclear events). Thus, a backup plan or system in which unexpected local demands (e.g., as people reroute their communications away from damaged facilities) can be accommodated as part of a nationwide communications fabric are preferred. Space-based capabilities (e.g., in extant VSAT networks to geosynchronous satellites) have some

[6] For example, if a public ATM (UBR) service were used to implement the paths in DOJ's IP network, it could be susceptible to an Internet link saturation attack if it shared a physical facility with the Internet.

very attractive features and merits aggressive pursuit. That noted, because of limited transmission capacity, many large emergencies will require limiting capacity utilization to the most critical applications.

DOJ's strategy is therefore to plan on an IP-based WAN and investigate the relative economies and security implications of private versus public solutions to security issues (a private solution would have to include sufficient peering points). The plan includes the active pursuit of space-based backup.

Precision Security

Notwithstanding the many dimensions of security (e.g., ensuring hackers do not control system functions), precision security is the art of ensuring that read and write privileges to information are strictly limited to those people specifically authorized to do so. Precision security is an important component of information sharing and collaboration; without ironclad assurances that the circulation of information is limited, many DOJ components will not share with others – and deservedly so.

State of the Art and Current Trends

DOJ requires secure information systems having four main elements:

- *Authentication*: the ability to ensure that transmissions and messages, and their originators, are authentic, and that a recipient is eligible to receive specific categories of information;

- *Data integrity*: to ensure that data are unchanged from their source and have not been accidentally or maliciously altered;

- *Nonrepudiation*: to ensure that strong and substantial evidence is available to the sender of data that the data have been delivered (with the cooperation of the recipient), and, to the recipient, of the sender's identity, sufficient to prevent either from successfully denying having sent or received the data. This includes the ability of a third party to verify the integrity and origin of the data;

- *Confidentiality*: to ensure that information can be read only by authorized entities.[7]

The phrase "precision security" stresses the need for a system in which individuals take on one or more *roles* within the organization that bring with them certain access *privileges*, but in a dynamic environment in which roles and responsibilities change, requiring information access privileges to be revised promptly.

[7] These definitions and other portions of the discussion in this section are taken from Neu, Anderson, and Bikson (1999) *Sending Your Government a Message: E-Mail Communication Between Citizens and Government*. RAND MR-1095-MF, Chapter 5.

Appendix B
The Prospects for Technology Insertion White Paper

The standard way to provide precision security is to adopt a public key infrastructure (PKI) system. Such a system would be defined within a single organization but permit specific other individuals (e.g., within other government organizations, or cooperating foreign government agencies, or private sector organizations involved in a legal case or other DOJ matter) to participate on a limited, specific basis.

PKI systems, although once quite exotic, are now available as commercial off-the-shelf systems (COTS) by providers such as RSA Security Inc. (http://www.rsasecurity.com), Verisign Inc. (http://www.verisign.com), and CertCo Inc. (http://www.certco.com).

PKI systems provide each user with one or more key pairs: a public key known to the user's correspondents, and a private key known only to the user. These keys can be used as encryption keys (to ensure the confidentiality of messages) or as signing keys (to confirm the identity of the sender). Such systems provide certificate authorities (CAs), which are trusted organizations (e.g., an agency given this responsibility within the DOJ) that "certifies" that a particular public key is associated with a specific user. Such a CA would demand proof of identity before issuing a digital certificate binding a public key to a user. The CA must also provide such services as replacing certificates that have been lost or compromised, publishing directories of public keys, and assisting users.

Within a PKI, it is common to distinguish between identity certificates (described above), and authority certificates that grant an individual user specific information access or other well-defined authorities.

A substantial survey of PKI systems is outside the scope of this appendix. However, there are many reference texts available with descriptions of PKI systems. Among them are a report by the Computer Science and Telecommunications Board of the National Research Council (1996)[8], and a more technical treatment in Schneier (1996)[9]

There exists a Federal PKI Steering Committee located within the General Services Administration. The mission of this committee (see www.cio.gov/fpkisc) is:

> ... to provide clear, strong leadership within the U.S. Federal Government during the development and implementation phases of the Federal PKI. The Federal PKI Steering Committee will provide guidance and assist in the development of an interoperable public key infrastructure that utilizes commercial-off-the-shelf, standards-based products and services for a myriad of applications with a goal toward ensuring standards-based approval. However, it is recognized that certain unique applications may require that modifications be made to commercial products. The Steering Committee will: Identify Federal Government PKI requirements,

[8] Computer Science and Telecommunications Board, National Research Council (1996) *Cryptography's Role in Securing the Information Society*. National Academy Press.
[9] Schneier, Bruce (1996) *Applied Cryptography*, second edition. New York: John Wiley & Sons.

recommend policies, procedures and standards development activities that support a Federal PKI, provide oversight of PKI activities in Federal PKI pilot projects, provide oversight and guidance on the establishment of key recovery techniques, specify technologies needed for a Federal PKI, establish and maintain liaison with appropriate communities of interest, establish interoperability and security requirements of products and protocols related to the Federal PKI, and make recommendations regarding establishment, demonstration, and operation of a Federal PKI.

Perhaps the most significant adopter of PKI systems for information security within the U.S. government is the DoD. The Defense Information Systems Agency (DISA) is coordinating these developments.

Due to the importance of information security throughout DOJ operations and agencies, we expect that DOJ would be an *early adopter* of PKI technology, obtaining support and guidance from the Federal PKI Steering Committee to assure that its systems were compatible with other U.S. government PKI initiatives. The "adopter" role is appropriate because PKI security is available in various relevant forms from a variety of commercial providers. It would seem most likely that the DOJ would desire to retain certificate authority procedures in-house, although the administrative burden of issuing, verifying, and revoking certificates as needed – as well as providing user training, education, and help facilities – can be substantial.

How Can Technology be Used

The fundamental requirement for precision security is the ability to recognize specific individuals and accord them their proper access privileges. Given the difficulties of passwords (e.g., they may be easily guessed or accidentally revealed), true security requires either a biometric or a token-based device. This, in turn, requires that access to SBU data be accessed only through machines capable of reading tokens or obtaining biometric information. The existence of PCMCIA cards or "memory sticks" for palmtops suggests that such devices do exist. Alternatively, the same digital fingerprint capturing devices employed as part of JABS may be available to double as authentication devices to SBU systems. Access privileges authenticated in that way can then be applied to specific collaboration environments and case files. In support of such devices, DOJ in particular, and the law-enforcement community in general would develop an infrastructure of public keys (PKI).

Software aside, administration has always been the major challenge in the practical implementation of public key systems. If the system is too small, then it will have to handle too many exceptions; if it is too large, then a complex arrangement of key servers trusting other key servers will be necessary. Although issuing keys is straightforward (access lists can be created one-at-a-time, as administrators require), revoking them requires a detailed review to find which systems have to be alerted. Until that far-off day when a global and trusted public key infrastructure exists, DOJ would concentrate on the requirements of the nation's law-enforcement community: federal law-enforcement agencies plus selected counterparts, from foreign, state, local, and tribal governments (with the participation of the intelligence community to be determined). This would be a total population unlikely to exceed 200,000 -- well within the capabilities of a single (albeit well backed up) server. At its steady-state, such a system might have to issue as well as revoke roughly a hundred keys a day; again, no larger than a single office could deal with.