The Government Open Systems Interconnection Profile (GOSIP)

In this report:

Synopsis

Editor's Note

The Government Open Systems Interconnection Profile (GOSIP) specifies International Organization for Standardization (ISO) OSI-based data communications standards for connecting all types of computers, peripherals, and networks to support their interoperability.

Conformance to GOSIP's guidelines for all new computer systems purchased by the government, made mandatory in August 1990, marked the beginning of a new era of federal government computing. As a federal information processing standard (FIPS), GOSIP is not only forcing into retirement TCP/IP, an internetworking solution widely used by the government for years, it is also forcing potential federal government vendors to supply OSI-based products.

GOSIP specifications will be updated every year. Version 1.0 of GOSIP, currently in effect, calls for two OSI applications standards: X.400 for electronic messaging and File Transfer, Access, and Management (FTAM) for file transfer. Future versions of GOSIP will enforce standards for such capabilities as automatic data routing, connection-oriented service, directory services (X.500), document creation and document swapping, electronic data interchange (EDI), ISDN network access, and terminal emulation.

Distributed processing requires more than just a standard means of data communications. It requires standardization of the operating system and software applications portability. The Portable Operating System Interface for Computer Environments (POSIX) and the Applications Portability Profile (APP) will fill these needs. POSIX specifies a vendor-independent interface between a software application and an operating system. APP goes beyond the operating system, addressing networking, database, and user interface issues crucial to portable applications.

—By Martin Dintzis
Assistant Editor

Analysis

As computer technology grabbed the business world by the lapels in the 1960s and 1970s, large mainframe computers took over many traditionally manual tasks, such as number crunching and word processing. Users found computer storage both tidier and more organized.

It did not take long, however, for users to realize that computers could do more than just process mounds of data. Users explored ways of sharing computer-generated data and software with each other, marking the beginning of computer networking.

Computing at that time was expensive. Users relied on batch processing or timesharing mainframe computers through remote processing. Before Apple and the microcomputer, computer networking meant connecting the product line of a single vendor (such as IBM, which dominated both commercial and federal markets). In 1974, IBM developed a networking architecture for its products called Systems Network Architecture (SNA), which—despite its proprietary nature—planted the seed for connectivity. SNA today remains the most prevalent networking architecture in the industry.

The emergence of microcomputers and the establishment of proprietary networks left many users stranded on islands of automation. They had plenty of data and applications, but no means to share information among incompatible systems. In response came the concept of internetworking.

In 1981, Xerox Corp. moved the technology toward interconnecting different networks with the Xerox Networking System (XNS), a complicated set of internetworking protocols influencing the development of the OSI model. XNS never really caught on, however, and was later surpassed by a set of Department of Defense (DOD) internetworking protocols called the Transmission Control Protocol/Internet Protocol (TCP/IP).

The idea for TCP/IP arose in the early 1970s, when the DoD—under budgetary constraints—desperately needed a means of exchanging data with the research and development community. To meet those needs, it attempted to design a de facto networking standard called the Network Control Program (NCP). NCP specified the first set of protocols for connecting computers and peripherals on one network. Ten years after it first developed NCP, the DoD replaced its single-network architecture with the multiple-network architecture of TCP/IP. TCP/IP was being used for the DoD's Arpanet network by 1983.

TCP/IP not only added internetworking capability but also transferred data integrity checking from the network protocols to the host computer system. This transferal provides a more trustworthy system than NCP, which relied on the network for end-to-end transmission reliability. Today, TCP/IP's primary users include the federal government, universities, and research groups.

TCP/IP

A layered approach to internetworking, TCP/IP began as an experimental alternative to the DoD's packet switched network, Arpanet. TCP/IP contains four layers of exchange protocols: the network access layer, the Internet Protocol (IP), the Transmission Control Protocol (TCP), and the applications themselves (see Figure 1).

The *network access layer* sends data between two processors on the same network. The protocols used depend on the type of network, such as an X.25 packet switched network or an IEEE 802.3 CSMA/CD, 802.4 token bus, or 802.5 token-ring local area network (LAN).

The *IP layer* routes data among multiple networks, whether they are similar or dissimilar. The IP layer is where true connection among different networks occurs.

Figure 1.
Transmission Control Protocol/Internet Protocol (TCP/IP) Layers

Layer 4	Applications: SMTP, FTP, Telnet
Layer 3	Transmission Control Protocol (TCP)
Layer 2	Internet Protocol (IP)
Layer 1	Network Access

The *TCP layer* ensures that the data sent is in sequence and error free. It is often called the reliability layer of TCP/IP; the IP randomly sends data without monitoring the transmission.

At the *application layer* of TCP/IP, three protocols are available: the File Transfer Protocol (FTP), the Simple Mail Transfer Protocol (SMTP), and Telnet. FTP transfers files from one host to another, and SMTP sends electronic messages between hosts. The Telnet application provides terminal emulation capability, allowing remote users to run applications as if they were directly connected to a host system.

Because TCP/IP is a static set of protocols with limited functionality and is not based on international standards, it eventually will be replaced by the emerging OSI protocol suite. OSI is an evolutionary, high-performance set of international data communications standards designed to be extended and manipulated for internetworking.

But because of TCP/IP's massive installed base, especially in the federal government, it must coexist with OSI for the near term. Industry experts maintain that TCP/IP-based products, because they are available and proven, will remain popular through the early 1990s.

What Is GOSIP?

GOSIP, driving the standardization of OSI protocols, is a federal government procurement document for computer and networking technology specifying OSI international and draft standards. As a federal information processing standard (FIPS), GOSIP is not only forcing TCP/IP into retirement, it is also forcing potential federal government vendors to supply OSI-based products.

Although GOSIP represents a departure from the federal government's traditional purchasing methods, it is a conservative approach. GOSIP specifies only OSI protocols having reached the final stages of standardization—a draft international standard (DIS) or international standard (IS). This way, vendors and users are not strapped with products based on protocols subject to change, making them obsolete with each protocol amendment.

To ensure interoperability, GOSIP is based on vendor agreements reached at the National Institute of Standards and Technology (NIST) Workshop for Implementors of Open Systems Interconnection, commonly called the NIST OSI Implementors Workshop. This workshop series, where prospective vendors determine how OSI protocols will be implemented, has yielded Versions 1.0 through 3.0 of the implementation agreements that form the core of GOSIP. The agreements ensure that each vendor develops OSI-based products in the same fashion, guaranteeing compatibility. Federal users also provide input to these vendor-adopted agreements.

As TCP/IP did in the 1980s, GOSIP will provide to federal users a newer, more functional set of internetworking standards in and beyond this decade. Unlike its predecessor, conformance of new products to GOSIP has been mandatory since August 1990. In contrast to TCP/IP, GOSIP is designed to remain compatible, preventing its obsolescence. New GOSIP versions will be incorporated gradually, so that users will be informed of upcoming standards and can prepare for their implementation.

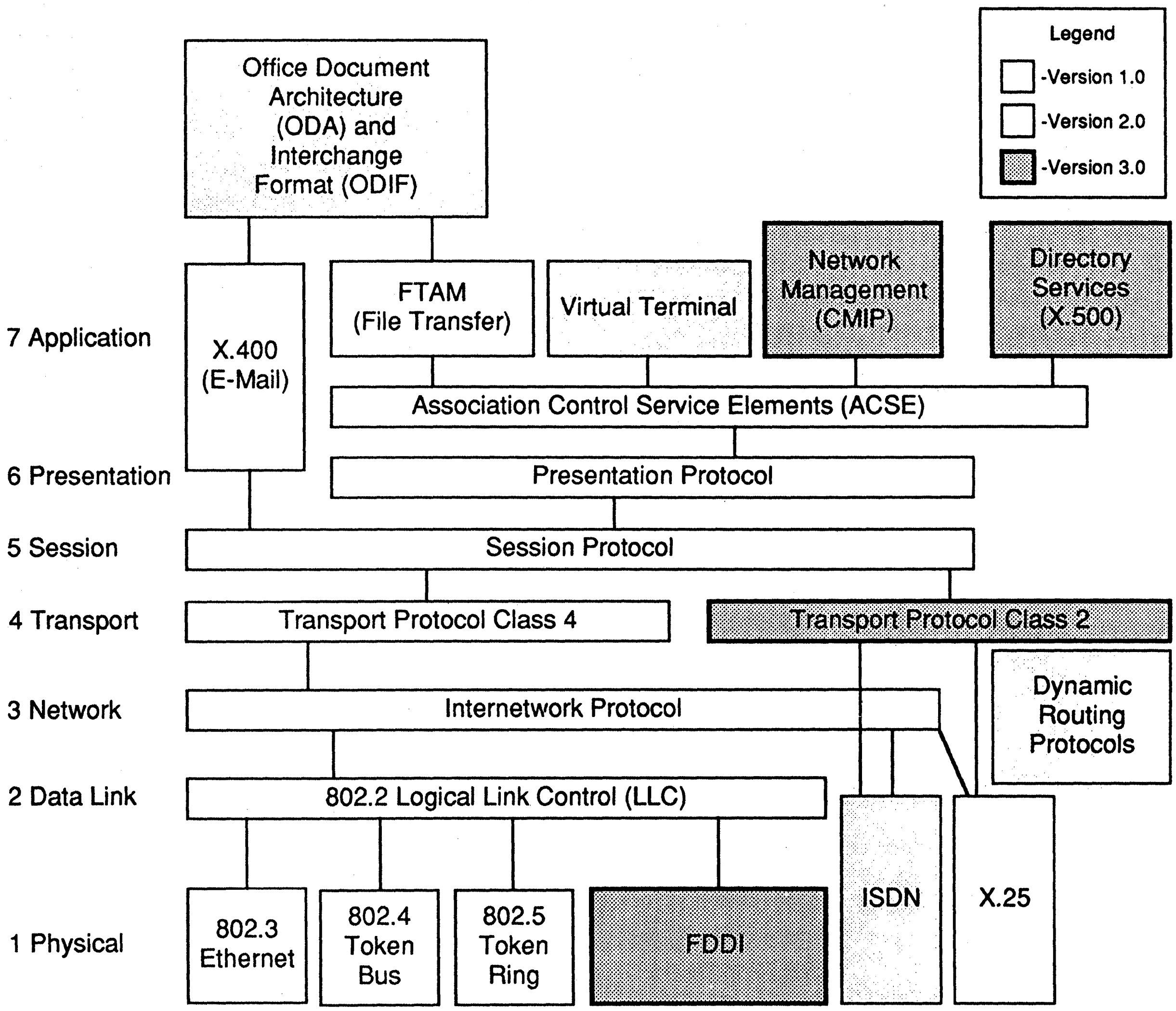
The continuity and worldwide standards approach of OSI and GOSIP will save the federal government in development costs. A 1985 National Research Council report estimated that commercial OSI-based products would save an average of 30 to 80 percent in information technology costs. No longer will government users be tied to a single vendor for networking and computing requirements. Instead, with OSI, they can select from a wide range of vendors, with the assurance that the products meet OSI criteria for connectivity.

OSI and GOSIP eliminate the need for expensive bridging and duplication of products, such as software and peripherals, which can be shared on a network. Standards let users preserve their product investments. GOSIP also provides procurement guidelines so that federal users can employ those OSI protocols in their purchasing decisions. Based on the seven-layer set of standards adopted by the worldwide standards body, the ISO, GOSIP contains only stable DIS or IS protocols.

GOSIP: A Layered Architecture

Version 1.0 of GOSIP, mandatory for new government purchases since August 1990, contains standard protocols at each of the seven OSI layers: physical, data link, network, transport, session, presentation, and application. These layers (see Figure 2) are often referenced by their placement in the OSI stack—layer one (physical), layer two

Figure 2.
GOSIP Protocols



(data link), layer three (network), layer four (transport), layer five (session), layer six (presentation), and layer seven (application). The lower layers, one through four, handle the interconnection of system processors on a network, while the upper layers, five through seven, interconnect the applications that run on those processors.

The Application Layer

The heart of the communications process, the Application Layer provides the interface between the network and the computer application, such as electronic messaging or file transfer. This is the layer nearest to the user, who wants to run software over various networks without learning the interworking of each OSI layer.

Thus far, GOSIP requires support for two OSI applications standards: the X.400 Message Handling System (MHS) for electronic messaging and File Transfer, Access and Management (FTAM) for file transfer. In addition, GOSIP mandates the Association Control Service Element (ACSE). ACSE is a service that corresponds to a particular application protocol, helping establish an association between the sending and receiving stations.

The Presentation Layer

The Presentation Layer plays the role of translator, converting transmitted data into a format understood by both sending and receiving systems. At this layer, GOSIP specifies the accepted OSI presentation protocol.

The Session Layer

The Session Layer establishes and synchronizes a communications session between application processors in a transmission. It sets up and closes the data dialog between those systems.

GOSIP merely calls for the OSI session protocol, suggesting that users select the various session functions based on characteristics of their own applications. Different applications require different session functions; therefore, the application drives the type of session function adopted.

The Transport Layer

The Transport Layer ensures that the data flowing between systems is sent intact to the proper destination. Sometimes called the "reliability" layer, Transport maintains the integrity of a data transmission. Transport Protocol Class 4 (TP4) is the OSI standard for transport and is required under GOSIP.

The Network Layer

The Network Layer determines the data's route. It sends data over various links to the destination system. GOSIP mandates the use of connectionless networking, provided by the OSI Connectionless Network Layer Protocol (CLNP), for networking between various subnetworks and within a single subnetwork.

The Data Link Layer

Here, the data sent from the Network Layer for transmission is packaged for travel over the network medium. GOSIP specifies Data Link Layer protocols, such as High Level Data Link Control (HDLC) for X.25 transmission and the LAN transmission protocols prescribed by the Institute of Electrical and Electronics Engineers (IEEE 802.3 [Carrier Sense, Multiple Access with Collision Detection, or CSMA/CD], 802.4 [token bus], and 802.5 [token ring]). The document also includes the protocol for the logical link, Logical Link Control (LLC).

The Physical Layer

At the Physical Layer, the physical connection is established. This layer contains the protocols for passing the bit streams across the transmission medium.

GOSIP does not mandate a specific physical interface standard but recommends the Consultative Committee on Telegraph and Telephone's (CCITT's) X.25 packet-switching protocol, standard interfaces such as EIA RS-232-C for transmission speeds up to 19.2K bps, and the CCITT V.35 interface for speeds that exceed 19.2K bps.

GOSIP's Evolution

As the ISO process evolves, so will GOSIP. With the help of NIST, the Technology and Advanced Requirements Group of the Government OSI Users Committee will update GOSIP on a regular basis, adding new OSI standards as they are completed.

GOSIP Version 2.0

The next version of GOSIP, Version 2.0, was finalized in September 1989 and will become mandatory in August 1991. GOSIP 2.0 expands the Application Layer and adds connection-oriented transmission service as an option for government networks. It brings three new application-layer standards to the GOSIP profile: Virtual Terminal (VT), the Office Document Architecture (ODA), and the Office Document Interchange Format (ODIF).

VT allows a PC or workstation to act as an IBM 3270-type terminal and to access mainframe data and applications. Users at a remote site can access and run mainframe applications from the desktop. Similar to TCP/IP's Telnet function, this protocol is in demand at the DoD, where terminal emulation is a popular feature.

ODA and ODIF are both options for swapping documents among dissimilar systems. ODA provides the standard for office document appearance, and ODIF is the transfer format. Together they are crucial to the exchange of compound documents, those generated by different word processing software and those produced by desktop publishing systems. ODA/ODIF should not be confused with Electronic Data Interchange (EDI), a protocol allowing users to swap business documents electronically.

GOSIP 2.0 also includes dynamic routing protocols, which provide automatic data routing capabilities for a network. Version 1.0 of GOSIP only calls for a static routing mechanism contained in a rigid routing table.

Also supported by GOSIP 2.0 are Integrated Services Digital Network (ISDN) communications standards, connection-oriented service, the connectionless transport protocol, and the end system-to-intermediate system protocol. ISDN provides a backbone network alternative to X.25 packet switched networks, adding the capability of combining voice, data, and video over the same circuit.

GOSIP Version 3.0

The third version of GOSIP, finalized in 1990 and scheduled to become mandatory in August 1992, will feature two new OSI applications: X.500 Directory Services and the OSI network management protocol, Common Management Information Protocol (CMIP).

Directory Services provides global directory assistance, as well as a database of electronic mail users. With Directory Services, users of the X.400 Message Handling System can access a wide database of other E-Mail users. CMIP is the protocol providing communications between computing devices and a central management station on a network. The OSI community, the TCP/IP community, and the OSI/Network Management Forum have all backed the adoption of CMIP for OSI network management.

GOSIP 3.0 will also include the Fiber Distributed Data Interface (FDDI), a fiber LAN standard that would allow federal users to implement high-speed, 100M bps, fiber optic backbone networks.

At the Transport Layer, GOSIP 3.0 will add an end system-to-intermediate system protocol called Transport Class 2 for connection-oriented service, where two systems could be considered part of a single, logical network. In Version 1.0, GOSIP calls for connectionless service, allowing one system to access another by establishing a store-and-forward messaging system. Connection-oriented service is considered more efficient for internetworking, because systems can communicate around the clock without establishing a connection and disconnection for every session.

Other Future Enhancements to GOSIP

In addition to the protocols slated for the first three versions of GOSIP, the federal government has other protocols planned, including the Graphical Kernel System (GKS), Computer Graphics Metafile (CGM), EDI, and Transaction Processing (TP).

Both GKS and CGM already exist as applications profiles in the Technical and Office Protocol (TOP) Version 3.0 specification. GKS lets users run graphics programs over different types of systems and contains a "toolbox" for programmers to develop two-dimensional graphics capabilities. CGM provides for the exchange of picture information among different computer graphics systems.

EDI, the transfer of electronic documents among suppliers and customers, is used by such divisions of the government as the Defense Logistics Agency and the U.S. Customs Service. GOSIP-based EDI will be modeled after the ANSI X12 standard, which is already in widespread commercial use. The federal government and the ISO community are exploring how to integrate EDI into GOSIP-based systems.

Still in the formative stages in the federal government is Transaction Processing (TP), an application most common in financial and retail services. TP tracks and updates customer transactions. NIST, the Internal Revenue Service, and the Defense Logistics Agency are currently studying the government's requirements for TP.

Security for OSI

The ISO does not yet specify security protocols for the OSI standard. It has devised an OSI Security Architecture, however, that spells out security features. GOSIP's appendixes include the OSI Security Architecture, giving federal procurement officials a framework when ordering secure communications equipment. Several security protocols remain under development at the ISO and within the industry. When those protocols become available, they will be reviewed as possible GOSIP components.

The OSI Security Architecture contains five basic features of secure networks:

1. Physical Security: The physical medium over which data is transmitted.
2. End-System Security: The protection of processors on a network.
3. Tamper Resistance: A means of guarding against computer hackers.
4. User Authentication: The verification of users and their access to data.

5. Trusted Functionality: The assurance of a secure system's reliability.

Guidance for the Nontechnical User

How do federal users acquiring networking equipment and building networks employ the GOSIP document and its specifications? With the help of a user's manual.

In March 1989, NIST released a GOSIP User's Guide for all levels of users—from manager to communications technician. For the nontechnical manager, the guide provides an explanation of GOSIP's benefits and positive effect on productivity. The guide also provides a tutorial and covers GOSIP's relationship to other federal government information processing efforts, such as the Federal Telecommunications Systems 2000 program, Computer-Aided Acquisition and Logistic Support (CALS), and the Secure Data Network System project at the National Security Agency (NSA).

The Portable Operating System Interface for Computer Environments (POSIX)

For a distributed processing environment to be fully open requires more than a standard means of data communications. A need also exists for standard operating systems and software. While OSI provides connectivity, it does not specify software portability. In response, NIST issued in September 1988 a Federal Information Processing Standard (FIPS) for the Portable Operating System Interface for Computer Environments (POSIX)—a specification for a vendor-independent interface between a software application and an operating system.

POSIX is an IEEE standard initially launched in 1981 by an organization composed of AT&T UNIX users. The IEEE has proposed that POSIX be included in the ISO's open systems effort.

Written in the C programming language, which provides simple portability among different hardware platforms, POSIX permits true applications portability. POSIX interface software can run over different operating systems, regardless of hardware.

Like OSI, POSIX will free government users from the bonds of a single vendor. Government users will have more options when procuring software and can preserve existing systems.

Although POSIX has been closely associated with UNIX because of UNIX' portability features, POSIX is operating system neutral. But how do GOSIP and POSIX work together?

The Applications Portability Profile (APP)

APP will bring GOSIP and POSIX together under one umbrella. The Applications Portability Profile, which was included in the POSIX FIPS appendix, picks up where POSIX leaves off: beyond the operating system.

NIST developed APP after federal officials realized that POSIX alone did not provide true applications portability. While POSIX provided the first step, it failed to address the networking, database, and user interface issues crucial to portable applications. Furthermore, while GOSIP specifies communications procedures for heterogeneous systems, it does not handle the interfaces between a network and the applications. It is these deficiencies which APP fills.

APP specifies software interfaces for operating system and networking services. With APP, developers can write portable software programs using those services. The programs can be moved across different computing platforms. GOSIP, POSIX, and APP provide federal users with a full complement of tools for developing open, distributed systems.

The APP "toolbox" for developing portable software applications includes the following elements (see Table 1):

- Operating System
- Database Management
- Data Interchange
- Network Services
- User Interface
- Programming Services

The **Operating System** element is POSIX, a vendor-independent interface between an operating system and a software application.

Database Management provides and maintains a dynamic bank of data accessible by all types of applications. APP specifies the Structured

Table 1. Elements of the Applications Portability Profile (APP)

Function	Elements
Operating Sytem	POSIX
Data Base Management	SQL IRDS
Data Interchange: -Business Graphics -Product Data -Document Processing	 CGM IGES SGML ODA/ODIF
Network Services: -Data Communications -File Management	 OSI NFS
User Interface	X Window System
Programming Services	C Cobol Fortran Ada Pascal

Query Language (SQL) database language and the Information Resource Dictionary Systems (IRDS) standard.

Data Interchange includes business graphics, product data, and document processing. In this area, APP and GOSIP overlap significantly. APP, like future versions of GOSIP, contains CGM for graphics and ODA/ODIF for document processing. (The GKS and PHIGS graphics standards will be implemented under Programming Services, discussed later.) APP, however, also contains the Standard Generalized Markup Language (SGML) for document processing and the Initial Graphics Exchange Specification (IGES) for exchanging product data.

Network Services specifies GOSIP for the interoperation of dissimilar systems over networks. In addition, APP requires a file management feature, to ensure proper sharing and monitoring of files in dissimilar systems. APP also specifies Sun Microsystems' protocol for file sharing, called Network File System (NFS).

The **User Interface** for portable software programs is the end user's view into the open network. Since there are different applications available to users, they need a consistent interface to ease access to those applications. APP calls for the X Window System user interface, developed by MIT.

Programming Services must also be portable in this open software and communications environment. APP initially offers the C programming language, known for its portability. To expand the programming language options, APP will also support Fortran, Cobol, Ada, and Pascal. The Graphical Kernel System (GKS) and Programmer's Hierarchical Interactive Graphics System (PHIGS) standards will also be supported in this section of the APP.

To support APP's evolution, NIST will sponsor user and implementor workshops similar to those it operates for OSI. The process for APP will be similar to NIST's OSI workshops, allowing vendors and users to provide input for implementing APP.

The Impact of GOSIP, POSIX, and APP on the Marketplace

Given the three elements of open distributed processing—GOSIP, POSIX, and APP—federal government users will have the tools necessary to forge ahead in computing. With the federal government's backing, standardization efforts will be a catalyst of open networking for the entire industry.

There are advantages and pitfalls to pioneering OSI and applications portability, however, and the federal government likely will be the first to experience them. The chore of ironing out new technology wrinkles is ever present. There is a learning curve caused by eliminating old, established information processing tools to make room for new techniques.

Being the first to adopt OSI means reaping the economic and functional benefits sooner than users who wait, a particular advantage for the federal government, which is constantly under budget constraints. OSI will help agencies tie together different computing and communications devices that currently cannot communicate. Once systems are connected, federal users can better exploit existing capabilities and easily add new standards-based technology.

POSIX and APP will enhance the communications capabilities inherent in GOSIP-based networks. With the strong backing of the U.S. federal government, these three information technology standards will more rapidly infiltrate the commercial market as well. Entering the fledgling OSI market via GOSIP guarantees advantages, but it also means risking interoperability troubles with latecomers' OSI products.

Despite pioneering risks, GOSIP will serve as a catalyst to entice vendors into developing OSI-based products now, rather than waiting for the market and technology to mature. GOSIP's federal government stamp of approval should alleviate the risks. Vendors that forge ahead with GOSIP products will be those wanting a share of the lucrative federal government computer and communications market. For smaller vendors, entering the OSI market in its infancy provides a foothold in what will become a massive market by the late 1990s.

The OSI market will be one where vendors supplying products based on the same standards must differentiate their offerings with added features, functions, or service. Vendors that join the market early can later devote resources to developing distinguishing features while latecomers are still buried with OSI research and development.

Because OSI is inevitable, industry experts feel all vendors will be forced to implement it within the next four years. OSI will yield a more competitive marketplace, where vendors will be unable to "lock" customers into their proprietary systems. Because compliance with GOSIP has been mandatory since August 1990, federal users now have access to a world of open internetworking, complete with greater software and hardware options and the capability to maintain their capital technology investments. Users not only will have more options in choosing their information technology tools, they also will be assured that the products operate under the same set of protocols. ■