GOSIP Overview

MLM-MU-91-71-0002

By Harrell J. Van Norman

INTRODUCTION

The U.S. Federal Government has mandated use of the International Standards Organization's Open Systems Interconnection (OSI) protocols throughout all federal computer network services and products. A Federal Information Processing Standard (FIPS) was adopted February 15, 1989 and enforcement began August 15, 1990. This FIPS describes, in publication 146, national policy mandating use of a functional profile of OSI approved protocols relevant to the federal government. Law requires all federal agencies purchasing network services and products to specify the Government OSI Profile, called GOSIP. This standard is compulsory and binding for all procurements of new networking products and services and for major upgrades to existing computer networks.

Since the Federal government is the largest single purchaser of networking components, the GOSIP specifications will generate significant impact within the data communications industry. GOSIP places no direct requirements upon non-Federal entities such as regional and local agencies, and non-public organizations. However, many agencies and organizations are moving toward GOSIP as their basis for transition to open systems.

Territorial boundaries and different languages are not the only things that separate countries. Rules by which computers communicate with each other vary from one country to another. This variation even extends to the Open Systems Interconnection (OSI) protocols, intended to provide a standard allowing computers to communicate across national as well as vendor lines. The volume of protocols included in OSI is so vast that no single product or user organization can support them all. Governments in several countries have defined or are defining a subset of the protocols they intend to use, called a government OSI profile or procurement, or a GOSIP. Besides the U.S., the U.K., Canada, France, Belgium, West Germany, Japan, Australia, Sweden and the Netherlands all have GOSIPs. Yet even these standards can diverge at layers 3 and 4 of the OSI model, with some based on connectionless protocols and others on connection-oriented protocols.

THE IMPACT OF GOSIP

GOSIP marks the beginning of a new era in Federal government computing policy. Information exchange has become an ever increasing factor in conducting business. Federal agencies share information with other federal agencies and with state and local governments and commercial organizations as well. Until recently, computer networking technology has not kept pace with these communication needs. Vendors continue to produce proprietary systems that are not interoperable in open systems. Today many Federal agencies have "islands" of computer systems built by different vendors or by the same vendor that cannot interoperate.

Standards-based telecommunications networking is gaining momentum as the Federal government has instituted the Government Open Systems Interconnection Profile (GOSIP). Federal government agencies, corporate networks, and vendors are all feeling the impact of GOSIP. All Federal agencies must require this subset of OSI internetworking protocols in their purchases of communications equipment. As of August 15, 1990, U.S. Federal agencies were mandated to procure network equipment conforming to the GOSIP standards. The GOSIP program is influencing purchase decisions in corporate networks as well, leading to a faster distribution of OSI throughout the networking community. Vendors must sell GOSIP-conformant products to get a part of the $22.5 billion in government procurement funds expected to be spent in fiscal 1992. Vendors are reducing their emphasis on proprietary products in favor of deploying OSI. GOSIP is bolstering availability of OSI applications, and leading to reductions in network expenses.

Is Compliance Really Necessary?

GOSIP must be cited in solicitations and contracts when systems to be acquired provide equivalent functionality to the protocols defined in the current GOSIP document. These requirements do not force replacement of any computer network service or product solely for GOSIP conformance. Whenever new computer network services/products are acquired or major upgrades are made to existing systems, these criteria must be considered. Additionally, many agencies have identified areas where GOSIP is desirable but where mandatory applicability is not required.

Three main reasons were used by the U.S. Federal government to justify GOSIP mandates. First, this law stimulates product development. Every computer and communications vendor is keenly aware of the tremendous market potential for GOSIP compliant products. The Federal government, as the largest single purchaser of communications network services, has significant influence on market trends. Impacting both systems directly procured by the federal government and in non-government support agencies striving to maintain a close alliance with federal government policies for computer and communications services. Requiring GOSIP protocols throughout all Federal agencies will result in development of a large quantity of OSI products. Today, there is only a smattering of certified OSI compliant products to choose from. The products that are available are not mature and fully tested for interoperability and conformance. However, in the coming months we can expect to see a flurry of activity from vendors announcing OSI based products. GOSIP is stimulating product development, yielding benefits to the entire industry.

A second motive for mandating GOSIP is reducing costs to acquire computer network services and products. Over the long-term, purchasing and installing GOSIP technology will minimize total investment costs and reduce conversion costs. Current GOSIP products are available at a relatively competitive price. A major benefit is that GOSIP will minimize total investment costs through extended life cycles, reduce conversion costs, and increase modularity. Thus, a smaller portion of networking budgets will be required for purchase and installation of GOSIP technology than for purchase and installation of alternative equipment. In other words, adopting GOSIP makes good economic sense.

The third reason for mandatory compliance is promoting the availability of interoperable and open systems. Standards alone won't assure interoperability. The OSI standards contain many more options than are practical to implement altogether. If each vendor only implements a subset of options, there is no guarantee that all vendors will implement the same subset. This can easily result in two products, each being fully standards compliant, yet not able to interoperate. GOSIP requires product certification testing for conformance and interoperability. This testing and registration of GOSIP compliant products ensures conformance and interoperability in a way standards by themselves never could.

THE GOSIP UMBRELLA

GOSIP, in addition to being a Federal mandate, is an alert that a nonproprietary communications solution has been developed. GOSIP is not only the first mandated protocol for all Federal government agencies, but it also marks the retirement of Transmission Control Protocol/Internet Protocol (TCP/IP), an internetworking approach widely used by the Federal government for years. Removing TCP/IP from the umbrella of preferred communications approaches is a significant redirection. TCP/IP, a four tiered layered communications architecture, is widely used by DOD's packet switching Arpanet. TCP/IP includes the physical network access layer, the internet protocol layer, the transmission control protocol layer and the applications layer supporting one of three protocols: the File Transfer Protocol (FTP), the Simple Mail Transfer Protocol (SMTP), and Telenet. Standardized GOSIP functionality is replacing the TCP/IP protocol suite.

New GOSIP versions are introduced every 12 to 18 months, reflecting progress made by vendors in providing OSI products with new services useful to federal agencies. Each new version supersedes previous versions because it includes every protocol in previous versions plus the additional new protocols, all under the GOSIP umbrella. All new versions are downwardly compatible with previous versions. GOSIP increases in scope as more standards reach a stable and mature status. OSI only considers including stable and mature OSI protocols, ones that have reached the final stages of standardization as a Draft International Standard (DIS) or full International Standard (IS). This ensures vendors and users are not strapped with products based on protocols subject to change.

Occasionally, changes are made to correct errors and to align with activity in international standards organizations.

GOSIP Version 1 included two major features: X.400 for electronic mail; and File Transfer, Access and Management (FTAM) for file transfer capabilities. GOSIP Version 2 is now adopted and includes Virtual Terminal, Office Document Architecture, and Integrated Services Digital Networks.

GOSIP and the OSI Reference Model

The International Organization for Standardization (ISO) formally initiated the Open Systems Interconnection Reference Model March, 1977, in response to the international need for an open set of communications standards. OSI's objectives were to allow internetworking between interoperable, multi-vendor networks. The U.S. government chose OSI because it is an international standard supported by the U.K., Canada and many European countries. Of primary importance is information exchange and interoperability on an international level. The OSI Reference Model is similar in structure to that of IBM's Systems Network Architecture. It consists of seven architectural layers: the physical layer; the data link layer, the network layer; the transport layer; the session layer; the presentation layer; the application layer. Generally, the top three layers are responsible for processing information, the middle layer ensures proper delivery of the information sent, and the bottom three layers provide a vehicle for physically transferring information from one system to another.

GOSIP is based on Stable Implementation Agreements for Open Systems Interconnection Protocols reached at the National Institute of Standards and Technology (NIST) Workshop for Implementors of Open Systems Interconnection, commonly called the NIST OSI Implementors Workshop. Here, OSI functional profiles are produced by identifying options that must be supported and necessary implementation details outside the scope of the standards. GOSIP is an OSI functional profile based upon Stable Implementation Agreements generated at the quarterly NIST Workshop for Implementors of OSI. It reflects implementation specifications or Workshop Agreements reached by vendors and federal computer users. The agreements help to ensure compatibility between vendor developed OSI products. Each new version of GOSIP is approved and adopted 12 to 18 months before mandatory enforcement begins, allowing users to prepare for each stage of implementation.

Versions 1 & 2

GOSIP Version 1 included two application layer protocols: X.400 Message Handling System (MHS) and File Transfer, Access and Management (FTAM). Routing and reliable transfer of data is accomplished in version 1 through a single transport protocol class 4 and a Connectionless Network Layer Protocol (CNLP). Version 1 also supported interconnection of the following lower layer network topologies for local and wide area networking: CCITT Recommendation X.25; Carrier Sense Multiple Access with Collision Detection (IEEE 802.3); Token Bus (IEEE 802.4); and Token Ring (IEEE 802.5).

Version 1 provides application layer functionality to exchange electronic mail using the X.400 MHS standard. This protocol, formalized in 1984, provides a set of standards to ensure global connectivity for electronic mail and other messaging oriented information exchanges. Two fundamental types of message handling services are provided: a person-to-person communication of electronic mail, called Interpersonnal Messaging (IPM), and a generalized application-independent Message Transfer (MT). X.400 uses the Reliable Transfer Server (RTS) as the basis for passing information from application to application, expediting access to the session layer. Unlike pure OSI applications, RTS bypasses most of the presentation layer, calling directly on session layer services.

File Transfer Access and Management (FTAM) is an OSI application layer protocol providing basic file transfer capabilities between any two systems. For file transfer sessions there needs to be two FTAM implementations involved, one acting as an initiator and the other serving as a responder. The initiator starts the file transfer session with the responder either to send or receive files. To start file transfers the initiator and responder must have specified Network Service Access Point (NSAP) addresses, identifying a network layer entity on an OSI network.

GOSIP version 2 was adopted April 1991 with October 1992 the date for mandatory enforcement. Version 2 includes all Version 1 functionality plus the following protocols: Virtual Terminal (telenet profile and forms profile), Office Document Architecture, Integrated Services Digital Network (ISDN), and End System to Intermediate System routing protocol (ES-IS).

GOSIP 2.0 provides options for network managers to consider in their purchases including security features and provisions of Connectionless Transport Service (CLTS), and Connection-Oriented Network Service (CONS). CLTS is to be used for internetworking of concatenated subnetworks and for operation of a single logical subnetwork. CONS is an optional service that may be specified for end systems that are directly connected to X.25 networks. CONS can lower the overhead associated with CLTS and may permit interoperation of systems that do not comply with GOSIP. CLTS and CONS were both included to allow for network efficiencies and easy integration in different levels of technology.

Office Document Architecture (ODA) and remote terminal access capability using the Virtual Terminal protocol is the expanded application layer functionality found in version 2. Virtual Terminal allows a PC or workstation to act as an IBM 3270-type terminal and access mainframe data and applications. Users at remote sites can access and run mainframe applications. Similar to TCP/IP's telenet function, Virtual Terminal is in demand wherever terminal emulation is a popular feature. Two categories of Virtual Terminal are defined: 1) simple systems providing functionality of a TTY compatible device and 2) forms capable systems supporting forms-based applications with cursor movement, erase screen, and field protection functions.

Office Document Architecture allows document exchange among dissimilar systems. It provides a standard for office document appearance and transfer formats, describing the logical and layout of documents as well as rules for specifying character, raster, and geometric content of documents.

ODA specifies a NIST Document Application Profile (DAP) where each word/text processing system includes appropriate system-to-DAP and DAP-to-system translators. This protocol should not be confused with Electronic Data Interchange (EDI), a protocol allowing users to transfer business documents electronically. Figure 1 illustrates GOSIP Version 2 architecture and protocols.

Versions 3, 4, and Beyond

Version 3 & 4 are not as stable, however, considerable long range planing has been done. X.500 Directory Services, Virtual Terminal (page & scroll profiles), MHS 1988 Extensions, FTAM Extensions, and Fiber Distributed Data Interface (FDDI) are scheduled for version 3, to be required about 4th quarter 1993. In 1995, Version 4 is anticipated to include Transaction Processing (to be used by agencies such as the IRS and the Department of Defense), Remote Data Base Access, Electronic Data Interchange (EDI), and possibly Synchronous Optical Network (SONET). Subsequent GOSIP versions will include those protocols developed by OSI that reflect progress made by vendors in providing products with new services useful to federal agencies.

Network Management

OSI network management is based on the Common Management Information Protocol (CMIP) and the Common Management Information Services (CMIS) standards. CMIP and CMIS provide a flexible framework for control and exchange of management information. Several other standards have been developed to define managed objects, their corresponding attributes and their management functions.

NIST has developed a separate FIPS for network management called the Government Network Management Profile (GNMP). Network management was originally under the GOSIP umbrella, with the OSI/Network Management Forum driving much of the specification efforts. The Forum has dropped the OSI portion of their name, reflecting an increasing emphasis on non-OSI network management solutions. The Forum encourages using OSI management on existing networks (like those based on TCP/IP), however, NIST believes this will result in interoperability and security problems. The security problem with using OSI on non-OSI transports is that a message encrypted at the transport level of a protocol stack will not necessarily arrive without the encryption being stripped off. GNMP calls for systems, applications and network management as well as database management. It recommends the Simple Network Management Protocol (SNMP) be used because the Federal government needs more than just OSI to manage its networks. GNMP will likely not be official until sometime in 1994.

Unified Standards

Four major OSI standard profiles are being merged into a unified OSI procurement document called the Industry Government Open Systems Specification (IGOSS). These OSI profiles, which are all subsets of OSI, are GOSIP, the Manufacturing Automation Protocol (MAP), the Technical and Office Protocol (TOP), and the Utility Communications Architecture (UCA). This will remove the confusion caused by multiple OSI profiles, all of which overlap to some degree. The consolidated document will be included in GOSIP 3.0, scheduled for April, 1992.

MANAGEMENT DIRECTION - Impacts to your organization

Each Federal organization implementing GOSIP needs to develop a migration strategy appropriate for their specific environment. No single strategy for integrating GOSIP compliant products with existing systems applies to all agencies. The most effective solution varies with current protocol architectures and configurations of existing systems. Some alternatives to consider include the use of dual protocol hosts, application and network layer gateways, and mixed protocol stacks. Refer to the Management Report "GOSIP Implementation Guidelines" MLM-MU-91-71-003 for specific implementation details. The long range objective is successful transition from today's computer systems and networks that are characterized by proprietary networking solutions to systems that are fully GOSIP compliant.

Several factors make it impractical to move immediately to full GOSIP compliance. Many agencies have considerable investments in existing computing systems and it is not technically or financially reasonable to move these systems to GOSIP in a single, all-encompassing changeover. Furthermore, today's products are limited and those that do exist are generally immature. Fiscal responsibility and good management practice encourage moving to GOSIP in an evolutionary fashion, not a revolutionary one.

Implementing GOSIP requires identifying four areas of responsibility: Acquisition Authority, Protection Authority, Name Registration Authority, and Address Registration Authority. All Federal agencies should identify individuals for each area of responsibility.

Most organizations have individuals performing comparable duties as Acquisition and Protection Authorities. However, Name and Address Registration Authorities are effectively new requirements and responsibilities to support GOSIP. These Authorities are identified and described below.

All Federal agencies implementing GOSIP need to identify an acquisition authority. This individual is responsible for issuing procurement requests for GOSIP standard-based applications operating over networks using GOSIP standard-based protocols. The acquisition authority also must specify performance requirements as a function of the source end system, the destination end system, and the communications links, subnetworks, and intermediate systems between the two end systems. Identifying procurements that are applicable to GOSIP and including GOSIP functionality in procurement specifications are the acquisition authority's responsibility.

Protection Authorities are necessary within GOSIP to define protection rules for an agency's security data. Security requirements for systems implementing GOSIP are identified and specified in the procurement document by the protection authority.

Address Registration Authorities are responsible for assigning and registering addresses used to identify specific components of the network. GOSIP's network addressing scheme is intended to uniquely identify each end system in the network in order to route data to it. Addresses are called Network Service Access Points (NSAPs). General Services Administration (GSA) is the official authority designated to assign all NSAPs to government agencies.

Name Registration Authorities are the individuals responsible for registering objects within the globally unique identifiers for OSI objects. This level of authority also may be delegated to lower organizational layers.

END-USER CONSIDERATIONS - Evaluating GOSIP compatible products

Various tests determine if products conform to GOSIP requirements and can interoperate with other GOSIP implementations. The NIST National Voluntary Laboratory Accreditation Program (NVLAP) was developed to accredit outside GOSIP certification laboratories. Groups, such as the Corporation for Open Systems (COS), which work to bring open systems to the computer industry, provide testing services and work with other organizations to ensure products conform to OSI standards. Compliance testing involves ensuring conformance to standards and interoperability with other products in the marketplace. In addition to testing for GOSIP compliance, COS also promotes international conformance with Europe's Standards Promotion and Application Group (SPAG) and Japan's Promoting Conference for OSI (POSI).

NIST is looking to the Defense Communications Agency (DCA) for assistance in conformance testing GOSIP products, accrediting NVLAP test laboratories, and registering products for GOSIP compliance. DCA's Joint Interoperability Test Center (JITC) will maintain GOSIP publicly available product registers of GOSIP conformance and interoperability. These databases, available through dial-in access, contain information about GOSIP compliant products and the tools used to test these products.

VENDOR IMPACT

Vendors are developing strategies and product lines for migration to OSI and the GOSIP standards. Computer and communications equipment vendors are acquiring additional companies, reorganizing services and developing cooperative agreements with suppliers of complementary products to act as value-added resellers and providers of complete integrated computer systems. This is advantageous in an industry where open systems, standards and networks are becoming the norm. Relations with users become more complex as customers demand interoperability in multi-vendor systems. Buyers also want the ease and cost reductions from dealing with single suppliers and one-stop shopping.

IBM has pledged to move further along the road toward open standards by announcing it will support OSI standards for connections between its mainframes and machines made by other vendors. According to an IBM spokesman, "The basic message of this announcement is IBM intends to be fully compliant with the GOSIP standards which national governments demand before buying equipment." Among the OSI standards IBM has pledged to support are electronic mail, file transfer, directory services, LAN and WAN connectivity and protocols for network management. IBM has also announced that it will support the TCP/IP standard, which is the current defacto market standard for connecting systems. As TCP/IP is not OSI compliant and is an older technology, IBM has said it plans to help customers migrate from TCP/IP to OSI compliant alternatives. IBM included with their statement of intent, some related products such as an OSI messaging and file transfer program for its RS/6000 range of workstations running AIX, called ALX OSIMF/6000.

Many companies that have heavily invested in TCP/IP products must face difficult issues when transitioning to GOSIP. GOSIP products have been slow to appear. Additionally, the certification methods the industry uses are not fully adequate to assure interoperation of products. Transition to OSI will actually be driven by the GOSIP mandate.

STANDARDIZATION - The Long and Winding Road

Someday, the world may all speak the same open, standards-based language but today computers don't speak the same language and it will be well into the 21st century until open, standards based protocols become the primary language of all communications equipment. Efforts of standards bodies, like the ISO and the CCITT, have realized developing truly open, interoperative communications protocols is no small task.

First there is the process of developing the standards among a forum of competing equipment manufacturers. Conflicting ideas and the desire to develop standards that best accommodates existing communications architectures of the various manufacturers are often frustrating and extremely time consuming. Agreement on the formats and functions often becomes a political issue rather than merely technical. Instead of doing things the best way from a technology viewpoint time pressures often force compromises to be made. Nevertheless, after years of deliberations and a multitude of standards meetings, protocol definition documents do emerge that receive the blessing of the standards organizations. First as draft proposals, then becoming draft international standards, until finally these documents emerge as full fledged international standards.

Once protocol standards are fully developed, the process to achieve truly open, interoperative products has just begun. One company implementing the standards interprets the meaning of the protocol specification one way, another company a different way. For this reason, implementor's agreements address these areas of ambiguity.

To complete the multistage process of generating interoperable and open systems products, implementations according to the Implementation Agreements must be tested. Two forms of testing are necessary: Interoperability testing and Conformance testing.

NIST has issued a GOSIP test policy document specifying procedures for vendors to follow to insure that their GOSIP compliant products are interoperable with systems built by other vendors and conform to standard reference implementations. It is the vendor's responsibility to demonstrate GOSIP compliance through obtaining interoperability certification and conformance certification through the NVLAP. For example, file transfer systems must be on the NIST interoperability certification list and provide proof of compliance through passing the approved conformance tests administered by a NIST approved test center.

Conformance testing exercises products against certified reference implementations by executing a series of standard functions. Several NVLAP test centers have been accredited for GOSIP conformance testing. When a product is tested for conformance it must interoperate with a certified reference implementation. Conformance testing by itself is not adequate to ensure interoperable and open systems. These certified reference implementations are not placed in the user's environment and are not an implementation the end user will exercise.

Interoperability testing is another critical phase of the product certification process for demonstrating OSI compliance. Here two specific product implementations are exercised against each other by running a set of NIST interoperability test scripts. This pair-wise demonstration of functionality is conducted by two vendors and the results recorded in DCA's JITC GOSIP registers. For interoperability tests conducted on the OSInet, the results are available through a free test and registration database maintained by OSInet, an affiliate of COS.

NIST is publishing the results of both interoperability and conformance tests in the publicly available database maintained by DCA's JITC. If products are not on the GOSIP register, then these vendors should not claim GOSIP compliant products through advertising or marketing. Compliance can not be assumed until both conformance and interoperability tests are completed. This level of protocol validation would not occur without the driving force of GOSIP.

NIST says that initial protocol tests may be incomplete or even flawed. This means that users have no guarantee products implementing the GOSIP protocols are fully GOSIP-compliant. NIST recommends users get compatibility assurances from vendors. These testing problems should be resolved soon and a comprehensive set of tests will be in place for GOSIP version 2 testing. This shows how important protocol verification and validation is to ensure interoperability.

FUTURE OUTLOOK - Living in an OSI World

The growth of distributed processing is pushing the demand for internetworking, the ability to communicate across computer systems from different vendors and linking multiple dissimilar communications architectures. The leading non-proprietary internetworking solutions are the Transmission Control Protocol/Internet Protocol (TCP/IP) and the Open Systems Interconnection (OSI) standard, led by the X.400 and X.25 protocols. TCP/IP is well-established and products based on TCP/IP have been available for over 10 years. OSI offers a richer set of standards than TCP/IP (having just five protocols - file transfer, terminal emulation, electronic mail and basic transport and internet protocols). However, there is a dearth of OSI products and interoperability across vendors has not been adequately demonstrated. Many companies already have TCP/IP networks in place, and are expanding its functionality. In spite of this, industry experts predict that OSI will become the dominant standard over the next decade. Reasons for this include U.S. and European Open Systems Interconnection Profile requirements.

The fates of the Open Systems Interconnection (OSI) Model and Transmission Control Protocol/Internet Protocol (TCP/IP) standard networking protocols in the user community are uncertain. Many predict OSI as the eventual industry-wide standard, especially after an U.S. government announcement that all Federal and military networking procurements must conform to GOSIP.

CONCLUSION

In an unprecedented move by the U.S. government, a profile of OSI protocols has been required by law for all Federal agencies. GOSIP mandates, intended to create open, interoperable computing environments, are having a significant impact on the communications industry. Vendors are quickly developing products and certifying them for conformance and interoperability. Federal computer users are able to reduce long-term purchasing requirements due to the economic incentives GOSIP offers. The entire computer communications industry is seeing a wide-spread emphasis on standards and open architectures. GOSIP is a major driving force behind all these changes.

GOSIP is growing in scope as progress continues in the OSI standards bodies. Version 2 is in place today with draft version 3 and 4 already under development. Applications under the GOSIP umbrella include X.400 MHS E- Mail, FTAM, Virtual Terminal, and Office Document Architecture. Routing and data transfer is through connection-oriented or connectionless-oriented session and transport layer protocols. Transport interfaces are available for RS-232, V.35, CSMA/CD, Token Bus, Token Ring, and Integrated Services Digital Network. Future versions are scheduled to include X.500 Directory Services, Electronic Data Interchange, Fiber Distributed Data Interchange, Transaction Processing, Remote Database Access, and Network Management.

Significant redirection in communications interconnection strategies does not happen over-night. Federal agencies that have invested heavily in proprietary communications approaches will not transition to GOSIP in one all-encompassing changeover. Developing a migration

strategy is the first step to successful GOSIP transition. Identifying authorities for acquisition, protection, name registration, and address registration is another key step. It must be emphasized that GOSIP, as a procurement regulation, does not force replacement of any computer network service/product. GOSIP is not intended to obligate the replacement of computer network services/products solely for GOSIP conformance, however, when computer network services/products are being replaced these criteria must be considered.

End users should keep in mind adequate testing and certification are necessary to ensure usable products. Just because a vendor implements GOSIP standard protocol formats and functions into their product does not ensure it actually conforms to the specification or that it will talk to another product. Conformance testing and interoperability testing are both prerequisites for complete product certification. Until products are on the certified GOSIP register for conformance and interoperability, assuming GOSIP compliance is presumptuous.

Like it or not, GOSIP has been mandated by the Federal government. Living in an OSI world requires training to learn alternative migration strategies of dual protocol stacks and gateways, name and address registration, and certification testing techniques. Over the long-term GOSIP will minimize total investment costs and reduce conversion costs. This is due to increased competition among product suppliers, effective multi-vendor interoperability, and minimal additional networking related software development. Adoption of GOSIP makes good economic sense throughout extended operational life-cycles. Initial short-term overhead of training and dual protocol stacks or gateways should be greatly outweighed by the long-term cost savings.

Figure 1. *GOSIP Version 2 OSI Architecture*