

# GOSIP Protocols to be Used for Industry Bids

By LTCmdr. Kevin Ebel, USN, and Kevin Mills

All industry proposals to the federal government after August 1990 for new advanced automated information systems or for major improvements requiring network services must use specified computer communications protocols. These protocols are in the government open systems interconnection profile.

As the date draws closer for government open systems interconnection profile (GOSIP) to become the mandatory protocol suite, questions persist over whether industry and the Department of Defense (DOD) are ready for this change.

To enhance interoperability among existing computer networks, DOD established in 1983 a set of military standard data communications protocols. This standardization was the culmination of a significant research and development effort during the 1970s, marking a milestone in computer networking technology. However, along with the advantages of this accomplishment came a number of unexpected and unfortunate complications.

Vendors were slow in accepting these protocols, resulting in the initial implementation of the military standards being created and maintained solely under direct DOD financial support. The standards were specified in English language descriptions, which led to ambiguities and misinterpretations. Additionally, no means of ensuring conformance to the military standards existed, and mechanisms for determining multivendor interoperability were unavailable.

Although the United States submitted these standards to the North Atlantic Treaty Organization (NATO) as a proposal to achieve allied interoperability, the other nations did not accept them for various technical, economic and political considerations.

DOD, along with the rest of the U.S. government, and in conjunction with the NATO community, could foresee that the commercial industry international standards for open systems interconnection would provide the basis to attain interoperability. With this concept, DOD began contributing to the development of GOSIP.

## **Scope of the Specification**

GOSIP is a technical specification used to inform potential vendors that certain protocols are required to satisfy a procurement agency's needs for interoperable data communications. The initial version of GOSIP includes electronic mail and file transfer applications operating over three local area network technologies and wide area packet switched data networks. GOSIP also includes a standard end-to-end, reliable transport protocol to interconnect various networks.

Planned additions to GOSIP will provide a remote terminal log-on capability, transaction processing, directory service and office document interchange applications, as well as integrated services digital networks and the fiber distributed data interface, a 100- to 200-megabit campus network technology. Developments also are underway to include into GOSIP the supporting technology for network security, network management and dynamic routing.

GOSIP is based on international standards for open systems interconnection. The protocols also are based on subsequent implementation agreements reached within an open international forum, the National Institute of Standards and Technology workshop for open systems interconnection. With past federal information processing standards, the National Institute of Standards and Technology generally refined international standards or

selected options on its own. Open systems interconnection standards, however, are so significant and comprehensive that a high level of expertise is needed to reach intelligent refinements. Considerable room exists within the computer community for honest technical and economic disagreement.

Establishing an open international forum seemed the most effective means for reaching the necessary refinement to open systems interconnection standards. GOSIP specifies details reached through such a process, operated by both potential users and suppliers of the interconnection products.

GOSIP is complementary to similar industry specifications, such as the manufacturing automation protocols, the technical and office protocols and the corporation for open systems profile. All of these profiles are based on a set of stable implementation agreements published by the National Institute of Standards and Technology, and, therefore, they specify the same interoperable open systems protocols. The manufacturing and technical protocol specifications also include some protocols not yet agreed on as international standards. In areas where the GOSIP, manufacturing, technical and corporation system specifications intersect (about 80 percent of the areas), vendor products built to comply with one will comply with all. This creates an additional incentive for major vendors to produce open systems interconnection products based on the output of the National Institute of Standards and Technology workshop.

An initial specification group, composed of representatives from 20 federal agencies, ensured that GOSIP version 1.0 would meet the requirements of as many federal users as possible. Substantial technical contribu-

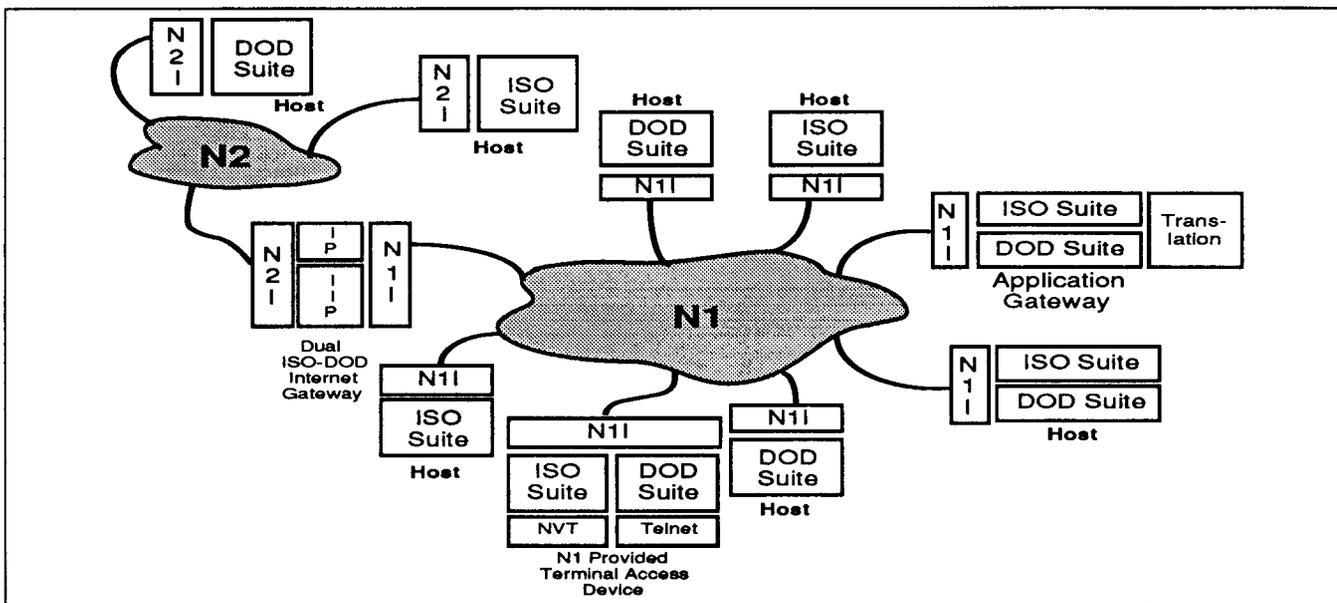


Figure 1. Department of Defense/open systems interconnection transition architecture.

tions from the National Institute of Standards and Technology, DOD, the Library of Congress, the National Science Foundation, the national communications system and the Department of Transportation resulted in a technically sound specification. While creating the first version of GOSIP, the initial specification group identified requirements for which open system protocols do not yet provide an available solution. A GOSIP advanced requirements group documented each such requirement, including a plan and schedule for including a solution into the system's profile. The advanced requirements group now is developing a second version of GOSIP.

### Financial Advantage

Saving money for federal computer users by enabling procurement of interoperable data communications products from a large set of vendors is the intent of the GOSIP effort. By citing a vendor-independent data communications standard, users can expect more bidders, leading to a better selection of cost, performance and function trade-offs. In addition, agencies specifying GOSIP can expect to upgrade hardware as technology improves without sacrificing data communications interoperability. Finally, gateways between proprietary communications architectures and open systems interconnection will enable agencies to adopt GOSIP on a time scale consistent with their schedule for planned upgrades and new acquisitions.

### Time Frame

GOSIP was approved as Federal Information Processing Standard (FIPS) Number 146 on August 15,

1988 and, beginning in August 1990, will be mandatory for the federal government. Several federal agencies already are experimenting with GOSIP compliant products. The National Institute of Standards and Technology manages an international multivendor network for open systems interoperability testing, with nodes across the United States, Europe and Australia. Several U.S. government agencies are connected to the network including the U.S. armed services, the National Aeronautics and Space Administration (NASA), the Defense Logistics Agency, the Department of Agriculture and the Defense Communications Agency. GOSIP already is being cited in procurements within DOD agencies, the Department of Education, NASA and several state governments.

### DOD Commitment

DOD policy states that, whenever international standards are available and can be used to support military requirements, they will be implemented as rapidly as possible to obtain maximum economic and interoperability benefits. In February 1985, the National Research Council (NRC) issued a report recommending that DOD adopt the open systems standards in lieu of the existing DOD standard protocols. As a direct result of the NRC recommendation, DOD worked with the National Institute of Standards and Technology to develop an initial draft GOSIP specification. A group of 22 federal agency representatives approved the specification in April 1987. Subsequently, the specification was proposed as a FIPS. In July 1987, the Office of the Secretary of Defense issued a memorandum

declaring open systems interconnection protocols specified in GOSIP as experimental co-standards with the DOD protocols.

With the adoption of GOSIP as FIPS 146, the Defense Department issued a memorandum in December 1988 declaring the open systems protocols to be full co-standards to the DOD military standard protocols. After August, when the FIPS 146 mandate occurs, the GOSIP protocols will become the sole mandatory interoperable protocol suite for DOD; however, a capability for interoperability will be provided for the expected life of systems supporting the DOD protocols.

### Implementation

The DOD open systems implementation strategy provides a technically and economically feasible approach for network subscribers to acquire and employ open systems interconnection products at a pace consistent with their procurement and improvement plans. The implementation of the protocols within DOD networks requires no cutover date because the networks will support transmission of both open systems and DOD protocols and will enable continued interoperability between all subscribers via application gateway services. Therefore, the number of open systems interconnection subscribers will increase over time as the number of DOD protocol subscribers drops.

Figure 1 shows a small, but logically complete, DOD internetwork in the process of transition to open systems protocols. This drawing illustrates the technology required to accomplish implementation. A key component is a dual-suited internet gateway capable

of rou  
open s  
protoc  
can be  
capab  
hosts  
suppor  
inter  
scribe  
works  
and w  
ate a  
intern

Two  
are rec  
operat  
system  
First,  
vices  
to per  
and fi  
users  
wheth  
exam  
DOD  
electr  
before  
user o  
the ga  
and ac  
ond re  
access  
virtual  
net pr

of routing both DOD internet and open systems connectionless network protocol datagrams. Such gateways can be used to interconnect networks capable of supporting both types of hosts into internetworks capable of supporting both protocols. Dual-suited internet gateways are required on subscriber premises to connect local networks to DOD backbone networks and within the DOD backbone to create a dual-suited DOD/open systems internetwork.

Two other important components are required to permit continued interoperability between DOD and open systems interconnection protocols. First, application-level gateway services are required on the internetwork to permit electronic mail forwarding and file transfer between any two users regardless of protocol type, whether DOD or open systems. For example, a message from a user on a DOD host would pass through an electronic mail application gateway before proceeding to the destination user on an open systems host. Within the gateway, the appropriate protocol and address translation occurs. A second required user service is dial-up access supporting the open systems virtual terminal protocol with the Telnet profile. Such a service permits

dial-up users to access open systems hosts.

DOD foresees the requirement for supporting a limited number of file transfer and electronic mail application gateways and dial-up devices supporting the virtual terminal protocol. The expected availability of dual-suited hosts, and even the application gateways, within vendor product offerings will enable network subscribers to provide such services for themselves. DOD is encouraging the availability of such commercial offerings.

A number of network subscribers within the Defense Department research community rely on publicly available software distributed in the form of the Berkeley software distribution (BSD) UNIX. These users are not likely to switch to commercial products at a rapid rate, and yet DOD desires this significant population to benefit from the technology developed in support of open systems implementation. For these reasons, DOD is supporting a project to place open systems protocol implementations into the kernel of the BSD 4.4 UNIX. In addition, the department is supporting enhancements to the publicly available International Standards Organization Development Environment

(ISODE) software. The BSD and ISODE software also will be implemented to comply with the Portable Operating System for Computing Environment (FIPS 151). The resulting software will be tested using commercially available conformance systems, and it also will undergo interoperability testing with other open systems implementations from commercial vendors.

### Strategy

DOD open systems implementation strategy charts the transition from the current military standard data communications protocols to the open systems suite of networking protocols. The plan covers DOD networks and their subscribers, including subscriber hosts and subscriber local area networks directly attached to the defense data network (DDN), as well as other DOD networks that do not attach directly to DDN. The Internet-connected networks of non-DOD related agencies do not fall under this plan. The Advanced Research Projects Agency network also is not covered by this plan; however, for planning a similar open systems transition for other agency networks, specific sections of the DOD implementation strategy may be useful.

## DCA: 30 Years of Progress Fourth Annual Forecast to Industry



Presented By:  
in coordination with

Defense Communications Agency  
NOVA Chapter AFCEA

at the

Crystal Gateway Marriott Hotel  
Arlington, Virginia  
April 17 and 18, 1990

Keynote Speaker:

Honorable Richard Cheney, Secretary of Defense (Invited)

Special Features Include:

- ◆ Major DCA Programs Overview
- ◆ Networking with DCA Program Management
- ◆ Changing Communications Requirements, Europe
- ◆ Other Defense Agencies Contract Information

Registration Information Available From:

Doreen Jakubcak  
c/o Computer Sciences Corp  
(703) 641-2506



Circle 11 on Reader Service Card

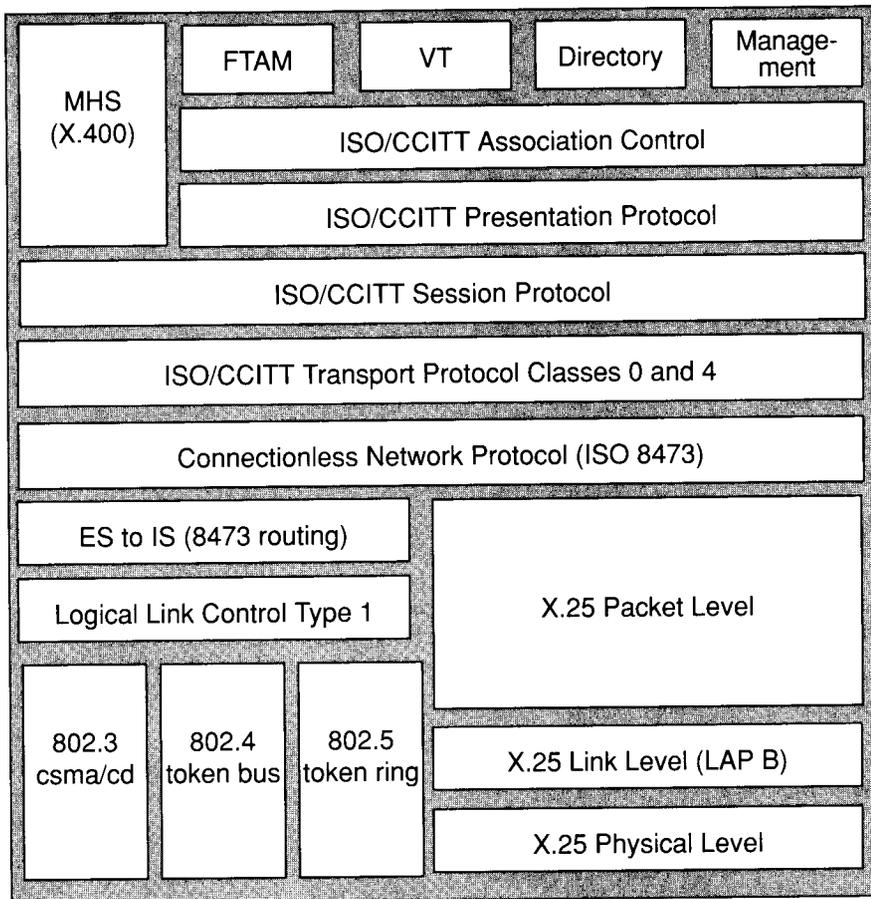


Figure 2. GOSIP protocol profile.

The DOD open systems strategy uses GOSIP as the governing document for specifying the open systems options and functions to be used. Areas currently defined as advanced requirements in GOSIP will be incorporated into future plans as they are added. The actual protocol profile to be implemented in end systems, along with some of the expected advanced requirements of GOSIP, are shown in Figure 2.

The availability of open systems products is a critical factor in scheduling interoperability and transition planning. A great deal of the open systems environment can be implemented from products currently available. Open systems implementations are commercially available from several equipment and software vendors to provide the equivalent functionality of existing services on DDN. However, future coordination of the open systems standards is required with product development and scheduling of future communication services. Internet gateway functionality also is required.

### Transition

For planning purposes, the transition from DOD to open systems is divided into two major categories:

The first implements open systems interconnection; the second covers DOD/open systems interoperability. Implementation deals specifically with deploying open systems products and services in existing or future DOD networks. Interoperability provides a capability for the military standard protocols on existing DOD networks to interoperate with the open systems protocols being introduced. DOD will support the existing protocols for the expected life of the systems using them. The transition plan will not impose an open systems cutover date.

By moving to the open systems networking protocols as the means for computers to interoperate in DOD, the potential for interoperability with comparable open systems in the NATO arena greatly is increased. Although both the United States and NATO are committed to using the international standards as the basis of their data communications protocols, the implementation of these standards may vary. The U.S. government open systems profile and the NATO open systems profile could become incompatible as they evolve; therefore, every effort should be made to prevent this and to achieve interoperability. The NATO Tri-Service Group on

Communications and Electronic Equipment subgroup on data processing and distribution, with the assistance of the Military Communications-Electronics Board, is working toward this goal.

DOD is committed to using computer communications protocols based on international industry standards to support military requirements. The need to achieve interconnection and interoperability of computers and systems now can be fulfilled by using the standards for open systems interconnection, instead of developing, testing and maintaining a unique set of military standard data communications protocols. DOD's use of commercially available products will lead to reduced costs by increasing the sources of supply and facilitating the use of advanced technology. Defense computer networking no longer will need to rely so heavily on proprietary solutions. DOD will continue to meet the needs of its extensive communications requirements by closely coordinating with efforts in the national, international and NATO standards arenas.

### References

- Government Open Systems Interconnection Profile (GOSIP), FIPS PUB 146, U.S. Department of Commerce, August 24, 1988.
- Gross, Phillip and Wilder, Richard. "The Department of Defense Open Systems Interconnection Implementation Strategy." The MITRE Corporation, May 1988.
- Mills, Kevin. "Government Open Systems Interconnection: Profile in Progress." Proceedings of ON-LINE OSI 1988. London, April 1988.
- Mulvenna, G., et al. "International Multivendor Interoperability Achieved Through OSINET." Enterprise Networking Event 1988. Society for Manufacturing Engineers, June 1988.
- National Research Council. "Executive Summary of the NRC Report on Transport Protocols for the Department of Defense Data Networks." National Research Council, February 1985.

. . . — . . .

*LTCmdr. Kevin Ebel, USN, is an electronics engineer at the Defense Communications Agency Interoperability and Standards Office, and is a member of the AFCEA Northern Virginia Chapter.*

*Kevin Mills is the division chief of Systems and Network Architecture Division, National Institute of Standards and Technology.*