DOE/ER/25188--T1

# Report of the Federal

# Internetworking Requirements Panel

## Prepared for the National Institute

## of Standards and Technology

## 31 May 1994

# Report of the Federal

# Internetworking Requirements Panel

## Prepared for the National Institute

## of Standards and Technology

## 31 May 1994

This document was prepared with the assistance of
The MITRE Corporation under Contract No. DAIAB07-94-C-H601

## DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

## TABLE OF CONTENTS

## PREFACE

The Federal Internetworking Requirements Panel (FIRP) was established by the National Institute of Standards and Technology (NIST) to reassess Federal requirements for open systems networks and to recommend policy on the Government's use of networking standards. The Panel was created at the request of the Office of Management and Budget in collaboration with the Federal Networking Council and the Federal Information Resources Management Policy Council. The Panel's membership and charter are contained in an appendix to this report.

Early in its deliberations, the Panel determined that the problems with the current situation were widely recognized, and that the most constructive strategy was to develop a revised approach to achieving Federal internetworking objectives as a basis for discussion. The Panel's draft report was released by NIST for public comment on 14 January 1994; comments were due by 18 February, 1994. A total of 77 comments were received, of which 19 were from outside the U.S. Comments from within the U.S. were received from 22 private sector organizations, from 8 Federal Government entities, and from 28 private individuals. The Panel appreciates the time and thought that went into the comments and thanks all the commenters. As a result of the comments, the Panel has refined and clarified its recommendations, and believes that its revised recommendations and supporting rationale provide the appropriate direction for Federal internetworking policy, process, and infrastructure. The Panel believes that the revisions address the major areas of concern while still meeting the practical need to include other standards in GOSIP.

# EXECUTIVE SUMMARY

The Federal Internetworking Requirements Panel (FIRP) was established by the National Institute of Standards and Technology (NIST) to reassess Federal requirements for open systems networks and to recommend policy on the Government's use of networking standards. The Panel was chartered to recommend actions which the Federal Government can take to address the short- and long-term issues of interworking and convergence of networking protocols - particularly the Internet Protocol Suite (IPS) and Open Systems Interconnection (OSI) protocol suite and, when appropriate, proprietary protocols. The Panel was created at the request of the Office of Management and Budget in collaboration with the Federal Networking Council and the Federal Information Resources Management Policy Council. The Panel's membership and charter are contained in an appendix to this report.

## Background

To meet requirements for data internetworking, the Federal Government in 1988 adopted Federal Information Processing Standard (FIPS) 146, Government Open Systems Interconnection Profile (GOSIP). The objective of GOSIP is to achieve interconnection and interoperability of computers and systems that are acquired from different manufacturers in an open systems environment. Beginning in 1990, GOSIP has been required by Federal Government agencies when acquiring computer networking products and services and communications systems or services that provide equivalent functionality to the protocols defined in GOSIP. Standards are added to GOSIP as requirements grow and products become available based on new standards. The current GOSIP Version 2 (FIPS 146-1) became effective in October 1992. The GOSIP standards were expected to displace the IPS and proprietary protocols because they were a result of the international standards process and were expected to be implemented worldwide.

## The Problem

In practice, some GOSIP products have been much slower in coming to market than expected and have not been widely deployed to date, while IPS standards have become commodity products that are widely used in LANs and private networks. More importantly, a substantial infrastructure, the worldwide Internet, has continued to develop which supports the IPS standards, while very little comparable infrastructure has been developed for GOSIP. Although there are finally a significant number of OSI products available, some are proving to be more costly and less integrated than equivalent IPS products. As a result of promoting GOSIP through procurement mandate, some agencies have acquired GOSIP-compliant hardware and software that is often not used or installed. In the meantime, agencies have continued to use proprietary solutions or have moved to adopt portions of the IPS.

Although the growth of IPS relative to the GOSIP protocols was the initial motivation for this policy review, other factors may be equally significant. These factors include: the continuing use of proprietary local area networks, the widespread deployment of proprietary electronic mail systems, the transition to client-server data processing architectures, and the continued dominance of proprietary communications architectures for mainframe based transaction processing.

In light of this reality, the Panel determined that it was necessary to review the entire strategy of meeting Federal Government internetworking requirements, rather than focus on the single issue of IPS versus GOSIP protocols. The sponsors of the Panel concurred

with this broadened scope. It must be emphasized that, in considering requirements, the Panel did not focus solely on data internetworking, since the trend is for data to be one component of multimedia information that may include voice, video, and image components. What is required is an effort to both take advantage of the capabilities now available and rapidly move developing capabilities into operational use. Many of the problems described above stem from too much faith that government-wide procurement standards could achieve the goal of Federal internetworking without a clear concern for mission objectives or cost realism.

## Conclusions

The Panel believes that the Federal internetworking standards process should focus on providing leadership to elucidate and then attain a common vision of how the Federal Government should be interconnected within itself and with the public. Then agencies should be held accountable for meeting their mission objectives in as compatible a way as practicable with that vision. Agencies should be given guidance in achieving interoperability goals via a broadened GOSIP consisting of protocols that are essential for core government-wide services and are mandatory for consideration for use.

The Panel concluded that no single protocol suite meets the full range of government requirements for data internetworking. Both the IPS and OSI protocols meet some needs, as do proprietary protocols in some situations. While a single standard would be preferable, the reality is that there are multiple solutions in networking as in other areas of information technology. The selection of standards for Federal use should consider various factors including interoperability needs, existing infrastructure, costs, marketplace products, and status as a standard. Agencies need a process that provides current guidance to assist them in deciding how to best meet their requirements, rather than the specification of technical solutions.

## Recommendations

The vision that the Panel sees for Federal internetworking is that it becomes a seamless component of the National Information Infrastructure, providing a full range of integrated communications connectivity among Federal agencies and between Federal agencies and the public and private sector. The Panel believes that the following recommendations are key to attaining this vision.

Recommendation 1. The role of oversight and guidance for integration across Federal agency internetworking activities should be strengthened.

Recommendation 2. The roles and responsibilities for fostering standards should be refocused and strengthened by the Department of Commerce.

Recommendation 3. The roles and responsibilities for infrastructure development and operations to support all internetworking services from advanced research and development to leading edge to core/commodity services should be clearly defined and formally assigned through the Information Infrastructure Task Force.

Recommendation 4. The roles and responsibilities of affinity groups should be defined, including how they are identified and coordinated by the Government Information Technology Services Working Group.

Recommendation 5. The current GOSIP policy should be replaced with a new FIPS that includes appropriate standards drawn from both the OSI and IPS protocol suites.

Recommendation 6. A permanent steering group should be established to review annually the Federal agencies' progress towards achieving the internetworking vision outlined in the Report. The existing FIRP Panel could also be made available to consult and coordinate with agencies working to implement the strategic and tactical recommendations of the report, to help ensure that the full vision of the report is accurately understood and communicated.

## 1.0 INTRODUCTION

The Panel was chartered to study issues and recommend actions which the Federal Government can take to address the short- and long-term issues of interworking and convergence of networking protocols – particularly the Internet Protocol Suite (IPS) and Open Systems Interconnection (OSI) protocol suite and, when appropriate, proprietary protocols. The overall Federal objective in internetworking is to achieve interoperability of applications services in addition to the lower level networking infrastructure within agencies, between agencies, and with outside organizations and the general public. The goal of Federal agencies is to use interoperability as an enabling infrastructure that will help them provide basic, common, relatively seamless sets of services to their users and improve the cost-effectiveness and reliability of their networking activities.

To meet requirements for data internetworking, the Federal Government began working on the Government Open Systems Interconnection Profile (GOSIP) in 1986. GOSIP was to provide a common set of standards for Federal interoperability and a process for adding to those standards, as requirements grew. The GOSIP standards were expected to displace the IPS because they were a result of the international standards process and were expected to be implemented worldwide. GOSIP standards had at least the functionality of their IPS equivalents available at that time.

In practice, some GOSIP standards have not been widely implemented to date, while the IPS standards have been. Probably more importantly, a substantial infrastructure has continued to develop which supports the IPS standards, while comparable infrastructure has not been developed for GOSIP. This reality, whatever the reason for it, has caused a review of the current policy on data internetworking.

Although the growth of the IPS relative to the GOSIP protocols was the cause of this policy review, other factors in the development of internetworking may be equally significant. These factors include: the continuing development of proprietary networking standards, particularly for local area networks (LANs); the development and widespread deployment of proprietary electronic mail systems, using graphical user interfaces on proprietary LANs; the transition to client-server data processing architectures; and major increases in the reliability and speed of both local and long distance digital transmission. In addition to these new factors, there is no real evidence of the imminent replacement of mainframe based transaction processing using proprietary communications architectures with anything from either GOSIP or IPS.

Many organizations within the Government and industry have evolved over the past twenty years to support a wide variety of computing capabilities and, correspondingly, networking services and protocols. Organizations continue to carry out their missions using a mixture of mainframe technology (with its centralized paradigm and terminal to host connections), minicomputers and workstations (with their peer-to-peer paradigm and LAN technology), and personal computers (with their client-server paradigm and proprietary workgroup LAN operating systems). Typically, large and medium sized organizations use all of these technologies. In addition, groups within an agency with responsibility for determining internetworking solutions need to have help when choosing the most appropriate internetworking technology to support the mission.

The result has frequently been a mixture of disconnected or loosely connected capabilities. Typically, organizations have attempted to stitch these various technologies together after the fact, where possible, to provide connectivity between different groups within the organization. The net result is often functionally disparate islands of technology connected through mechanisms and gateways that are unreliable, difficult to use, not understood by the vast majority of end users, and expensive to maintain.

## 1.1 BACKGROUND

**GOSIP.** Currently, Federal Information Processing Standard (FIPS) 146-1, the Government Open Systems Interconnection Profile (GOSIP), defines the official approach to Federal internetworking policy for data communications: "GOSIP shall be used by Federal Government agencies when acquiring computer networking products and services and communications systems or services that provide equivalent functionality to the protocols defined in the GOSIP. The objective of GOSIP is to achieve interconnection and interoperability of computers and systems that are acquired from different manufacturers in an open systems environment." (NIST, 1991)

GOSIP is based on the Open Systems Interconnection (OSI) protocol suite, which is a joint standardization program of the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU). The ISO and ITU standards are developed and approved by formal, widely accepted international processes, either by developing standards within ISO/ITU technical committees or by fast-tracking standards developed by other international and national bodies. The original GOSIP Version 1 became effective in August 1990. The current Version 2, which became effective in October 1992, includes more services: Virtual Terminal (VT), Office Document Architecture (ODA), and the End System to Intermediate System (ES-IS) routing protocol. At the lower layers, GOSIP embraces various network technologies: X.25, Local Area Networks (IEEE 802.3, 802.4, 802.5) and Integrated Services Digital Network (ISDN). GOSIP requires a full OSI stack, and does not endorse mixing and matching with other protocols. GOSIP Version 3, which is currently planned to be based on the forthcoming Industry-Government Open Systems Specification (IGOSS) Version 1, will have a relatively complete set of internetworking specifications, including Frame Relay, Directory Services, 1988 Message Handling Systems, and Intermediate System to Intermediate System (IS-IS) routing protocol.

**IPS.** The protocol suite based on the Internet Protocol (IP) and Transmission Control Protocol (TCP), which were developed within the U.S. military-funded research establishment and have since grown to become the basis of the worldwide Internet, is generally referred to as the TCP/IP Protocol Suite. The term Internet Protocol Suite (IPS) is used in this report to refer to the TCP/IP Protocol Suite for conciseness, since it is used in the Panel's charter, and to distinguish the full suite from the specific TCP and IP protocols. Standardization of the IPS is carried out by the Internet Engineering Task Force (IETF). The IETF process puts its emphasis and owes its success to the policy of "rough consensus and running code," which means that IETF members develop multiple, interoperable implementations of draft protocol specifications before they are declared as full Internet Standards. The IPS, although neither required nor precluded by GOSIP, is widely used by Federal agencies. Today there is significantly more actual interoperation within and between Federal agencies using IPS than using OSI standards, as well as between Federal agencies and the public.

**Internet.** The Internet is the system of interconnected computer networks that share the protocol suite and the name and address spaces that are specified by the Internet Architecture Board (IAB) of the Internet Society (Postel, October 1993; Reynolds, 1992). In February 1986, the Internet was primarily centered on the U.S. defense and research community with 328 registered networks, of which only 16 were non-U.S. (Lottor, 1993). As of December 1993, the Internet has grown into a huge international infrastructure of over 21,000 connected networks, of which over 9,000 are non-U.S., supporting an estimated 20 million users worldwide (Widmeyer, 1993). Compared with 1986, the Internet now connects 70 times more networks, with 45 percent of them non-U.S. as compared with about 5 percent in 1986. Also, there is today a significant commercial use of the Internet, whereas in 1986, commercial use was not permitted. The Internet now has a much more formalized standardization process than in 1986. Products that comply with IPS standards have now become commodities that are widely used in LANs and in private networks, in addition to their use on the Internet. At the same time, the Internet has become capable of supporting multiple protocols, including OSI, in parallel with IPS. In fact, the Internet now hosts one of the world's largest X.500 directory services pilots.

As the Internet infrastructure has grown up worldwide, its basis of success has also become more apparent. The Internet is not centrally controlled or managed by any single entity but is composed of a large number of networks run by a variety of organizations, including governmental, academic, research, and commercial organizations, ranging from user organizations to network providers. These organizations all cooperate informally to provide the interconnected service and to provide access for their own hosts and subnetworks attached to the network. Most of the hosts connect to the Internet using widely available commercial hardware and software, which comply with the IPS standards just by having to interoperate day-in and day-out in the open marketplace, and not because of any required Government test or mandate. The need to support this huge infrastructure and be able to transfer information over it drives the continuing development of new protocols, which in turn are deployed on the Internet, causing it to expand even more, and repeating the cycle as a new technology becomes widely available in products. The Internet has truly reached "critical mass," in the sense that a large and diverse set of organizations and even individuals must have Internet connectivity to do their jobs and are critically dependent on this infrastructure to obtain information.

Finally, with respect to the U.S. Federal Government and GOSIP: some Federal agencies, even while acquiring GOSIP-compliant technology, have played and continue to play a major role as users and developers of the Internet. Although the Government's share of funding for physical facilities of the Internet is declining dramatically, Federal Networking Council (FNC) agencies continue to support some of the vital infrastructural "glue" such as: administrative support for IETF meetings and the Internet Architecture Board (IAB), registration services, network information services, and directory and database services. FNC agencies also participate actively in the IETF standardization process, with a substantial number of active IETF participants being employed by, or supported by, the Federal Government. Federal agencies, contractors, and grantees, together, purchase massive amounts of IPS compliant hardware and software, far more than GOSIP. This is even more true in the commercial and private sector.

## 1.2 Current Situation

Organizations face many challenges in developing and implementing an enterprise-wide networking strategy that achieves economies of scale and provides an evolvable infrastructure for future applications that will support multimedia solutions. In decentralized organizations, it is often difficult to achieve the necessary level of consensus

within the organization on what this infrastructure should be, or that the infrastructure should exist at all. Even when consensus on technology is reached, there can be difficulties in developing an appropriate investment strategy. Frequently, different groups within an organization are responsible for developing and operating the network infrastructure and the applications that use the network. Various applications can require different network protocols. Furthermore, within a given type of application, such as e-mail, there can be many different packages running simultaneously within the network. The net result of these many layers of technical and organizational dependencies is that organizations can experience some degree of deadlock when they undertake enterprise-wide technology evolution, leading to the need for freedom in the transition process to tailor their approach to fit both the existing baseline and the target architecture.

When GOSIP was originally conceived in the mid-1980s, OSI products were beginning to appear, vendors were developing (and promising to develop) more products, and Governments and industries around the world were establishing plans and programs to adopt the OSI standards as the basis of their interworking. IPS products, on the other hand, were limited in the mid-1980s, and several major vendors of computer and networking equipment were still in a "wait and see" mode. The IPS standardization process was still largely informal.

By 1994, events have largely overtaken policy. First, most OSI products have turned out to be much slower in coming to market than expected. Although there are finally a significant number of products available, some (such as file transfer and virtual terminal) are proving to be less integrated than equivalent IPS products. In other areas (such as message handling and directory services), OSI products have become competitive with alternative offerings. A worldwide public carrier X.400 infrastructure has been put in place over an X.25 infrastructure, providing X.400 accessibility between almost all public service providers. Although the number of public carrier X.400 users worldwide is unknown, as an example, Compuserve has approximately 500,000 users. At the same time, the Internet has matured more rapidly and to a much greater extent than even its proponents expected.

Several agencies have implemented portions of GOSIP, mostly in the X.400 electronic mail area, with limited interagency interoperability. A lot of effort has been expended, but the bottom line is that today, even in electronic mail, interoperability across the Government is still only a goal. In limited communities, such as the Federal research community, e-mail interoperability is more widespread and treated as a utility using IPS.

During an era of declining budgets, there has been increasing pressure on Information Technology (IT) investment programs to clearly demonstrate added value and cost savings when acquiring new services. GOSIP has been promoted through procurement mandate, rather than through emphasis on how agencies can better accomplish their missions. This policy has led some agencies to expend a lot of effort to put GOSIP products on Federal procurements, but seldom buy any. In other cases, agencies pay GOSIP only lip service, acquiring GOSIP-compliant hardware and software that is often not used or installed. Products based on GOSIP versions 1 and 2 do not contain sufficient functionality. They are often poorly integrated since they are not subjected to the day-to-day rigors of widespread operational deployment. In the meantime, agencies have continued to use proprietary solutions or have moved to adopt portions of the IPS. By contrast, because of competition in the large marketplace, the IPS and proprietary suites are low cost and well integrated.

This current approach of paying only lip service to GOSIP has sent very mixed messages to vendors causing them to question the Government's intentions on GOSIP. Together

with slow acceptance in the commercial sector and the overall economic downturn over the past two years, this caused a number of vendors to slow their investment in developing some OSI products. In spite of this, over the past 12-18 months, a number of the key services in the planned GOSIP version 3 have become available in the marketplace, specifically Directory Services, 1988 Message Handling Systems, and the dynamic Intermediate System to Intermediate System (IS-IS) routing protocol. Today 1988 X.400 messaging products are available from many vendors, several X.500 directory service products are available, and IS-IS is available from major router vendors. The costs for messaging products are becoming competitive with both proprietary and Internet offerings.

The focus on "full stack" GOSIP at a time when the products were not widely available and deployed in large scale has undermined the use of just parts of the OSI protocol suite, even when potentially valuable parts of the OSI protocol family could be used over existing network and transport infrastructure. For example, X.500 Directory Services running over TCP/IP is not part of GOSIP Version 2, even though it is in use and could fulfill the needs for a Government-wide Directory.

### 1.3 Purpose

As stated in the charter, the Panel's objective is to study issues and recommend actions which the Federal Government can take to address the short- and long-term issues of internetworking and convergence of networking protocols - particularly the Internet Protocol Suite (IPS) and the Open Systems Interconnection (OSI) protocol suite, and where appropriate, proprietary protocols. The current GOSIP policy has as its primary objective "to achieve interconnection and interoperability of computers and systems that are acquired from different manufacturers in an open systems environment." However, GOSIP has not met its original objectives, and does not appear likely to in the near future. Events and the marketplace have evolved differently from what was expected when GOSIP was first conceived. The Panel was established to assess the current situation and to recommend a reality update in light of market conditions. The direction of GOSIP must be changed if the intent of GOSIP - to promote network interoperability - is to be realized.

The internetworking requirements of Federal agencies arise from their goal of meeting their mission needs while furthering overall Government interoperability objectives: intra-agency, inter-agency, and between Government and outside organizations. The challenge faced by the agencies is how to evolve their current, highly heterogeneous environments to an interoperable infrastructure that:

- meets their mission needs (often variable within a single organization)
- is affordable over its life cycle (relative to what they are now doing, or what is available in the marketplace, or what funds are available)
- reliably provides the desired levels of service to all users
- can evolve as new technology evolves in a manner that is cost effective and nondisruptive for users.

### 1.4 Approach and Scope

The Panel quickly came to the conclusion that the fundamental issues were broader than the technical issues of interoperability and convergence between the IPS and OSI. They include the changing nature of the standards process which has resulted in multiple standards-developing organizations, and the numerous capabilities in one protocol suite for

which there is no counterpart in the other suite. A procurement policy alone is inadequate without consideration of the marketplace products, government infrastructure, and costs. The Panel believes that one necessary component of a GOSIP program is a document providing guidance similar to that found in the current FIPS 146-1, but without the mandate of a specific protocol suite since no single protocol suite meets the full range of Government requirements. Consequently, the Panel has focused on the process, including a structure for identifying interoperability requirements (affinity groups), responsibilities for an integrated internetworking strategy and infrastructure development across agencies, and the criteria for selecting protocol standards to be included in a new approach to GOSIP. This broader scope than defined in the Panel's charter was addressed with the concurrence of the Panel's sponsors.

In light of the broadness of this challenge, it is appropriate to review the entire strategy of meeting Federal Government internetworking requirements, rather than focus on the single issue of IPS "versus" GOSIP protocols or on a data-only requirement/solution set. What is required is to come up with a recommended approach for Federal internetworking that will both take advantage of internetworking capabilities that are available in the marketplace today while remaining open to the use of future capabilities that are currently under development.

Many of the problems described above stem from too much faith that government-wide procurement standards could achieve the goal of Federal internetworking. The Panel believes that the previous approach to Federal interoperability fails to enlist the vitality and cost-consciousness that can come only from agencies focusing on their missions, and that standards-setting from the top should be aimed not at procurement mandates but at government-wide interoperability objectives.

The Panel believes that the Federal internetworking standards process should focus on providing leadership to elucidate and then attain a common vision of how the Federal Government should be interconnected within itself and with the public. Then the agencies should be held accountable for meeting their mission objectives while furthering the overall vision of Government-wide interoperability over a shared infrastructure.

The Panel divided its work into the general areas of Requirements, International Interoperability and Trade, Standards Process, Technical Issues, and Economic Considerations. This report reflects that structure of its deliberations. In this report, the Panel points out what it thinks are better directions for Federal internetworking in the areas of policy, process, and infrastructure, based on the Panel's perceptions and analyses of worldwide and U. S. Federal internetworking current realities and future trends.

## 2.0 REQUIREMENTS

Federal agencies have a wide range of internetworking requirements today and will have an even wider range of requirements in the future, as technology advances and the recommendations of the National Performance Review (NPR) (Gore, 1993) begin to be implemented. These requirements can be categorized in a number of different ways. These include functional modes of communications, such as conversational, messaging, transaction processing and information retrieval; characteristics, such as connectivity, interoperability and security; and communities of interest or affinity groups, distinguished by geographic proximity, shared interests or missions, or service providers and their customers. In considering requirements, the Panel did not focus solely on data internetworking, since the trend is for data to be one component of multimedia information that may include voice, video, and image components. Information should not be available just one way, but in a whole range of ways, and not just to Government employees, but to citizens being served by Government and to industry transacting business with the Government. An expanded discussion of Federal internetworking requirements is contained in (GSA, 1994).

### 2.1 Functional Modes

Functional modes of internetworking are differentiated by a number of specific technical communications features. These features include latency, acceptability of variability in delay, the number of endpoints for an information stream, the need for simultaneous availability of endpoints, and the expected duration of the information exchange. The following functional modes are identified.

**Conversational.** The conversational mode is characterized by a multiway (usually two way) unstructured exchange of information at roughly the pace of normal human conversation. Telephone calls are the classic example of this mode, and represent a high level of development in all of the characteristics required of a communications mode. Multimedia multipoint conferencing is the requirement which will most challenge technology, or constitute the "technology driver" for this mode of communications.

**Messaging.** The messaging mode, also known as store-and-forward, is characterized by an exchange of information in which one participant sends information to other participants with the expectation of some delay larger than that in a normal conversation in the delivery of the information. E-mail is a contemporary example of this mode. The technology driver for this mode is multimedia messaging. Users would like to be able to leave messages which include voice, image, data, and video components.

**Information Retrieval.** The information retrieval mode is characterized by a structured request for information from one party to a designated source of information. The classic example of this mode is directory assistance in the telephone system. The technology drivers for information retrieval are multimedia input requests (voice, data, or graphical user interface) into an up-to-date distributed information base which can provide multimedia responses.

**Broadcasting.** Broadcasting is characterized by the widespread dissemination of information without a specific request by the recipients. This communication is normally one-way. Broadcast radio and television are a classic example of this mode. Broadcast has been used when there is no requirement to guarantee that all possible recipients have received the information. The technology driver for this mode is wideband transmission

and cable systems which permit a wide range of information to be in "flow-by" mode for users, like the stock prices or weather reports, which the user's equipment can capture based on a stored profile. A variant of broadcast is multicast, where a number of recipients, but not all recipients, accessible by a particular communications system are sent information.

**Transactional.** The transactional mode is characterized by a structured request for either information or action by the requester, and a response containing the requested information or confirmation of the action. Examples are airline reservation systems and electronic funds transfer. The key characteristic of transactional mode is the concept of "indivisible, guaranteed action" that ties together all the pieces of the transaction into a single logical event. Electronic commerce depends on a combination of the transactional and messaging mode. In both the government and industry, transactional mode communications have been almost entirely supported by dedicated networks running proprietary protocols. An example of a technology driver is multimedia updates to electronic catalogs.

**Composite.** The composite mode involves communications consisting of a mixture of the above modes of communication. All modes would permit a range of media (voice, graphics, data, including highly formatted data such as documents and spreadsheets, and video) to be employed in the process. A single integrated workstation would support the entire composite mode requirements of the Government employee, and citizens could use whatever range of capabilities their personal communications equipment could support. Calendar and workflow software are examples which are beginning to be in widespread use. Examples of technology drivers are multimedia conferencing and virtual reality.

## 2.2 Characteristics

The following characteristics apply to some extent to all communications modes.

**Affordability.** Internetworking is affordable if it can be provided at acceptable cost. The cost has to be balanced against the perceived benefit and convenience.

**Connectivity.** A necessary but not sufficient requirement for internetworking is that the physical communications media of the internetworked components are "connected." The Federal Government also requires connectivity under other than normal conditions, for example, during emergencies, disasters, and war. Extensions beyond commercially provided services will continue to be needed for these requirements.

**Interoperability.** Interoperability is the ability for two systems to work together across a network. The degree to which useful work can be done in the internetworked environment versus the user's home network environment determines the degree of interoperability.

**Accountability.** Accountability is the ability to ensure that communication has taken place and was in the government's interest. In the internetworking context, this means that the responsibility for completion was transferred and is identifiable, the performance was met, the communication costs were appropriate and identifiable, and the use of the communication facility was in the government's interest.

**Cost Allocability.** Once costs have been accounted for, they must usually be allocated on some basis to the participants in the communication in accordance with OMB Circular A-130.

**Security**. There are security requirements for confidentiality; system and information integrity; sender and recipient identification, authentication, and access control; and sender and recipient non-repudiation. The needs for security contrast and usually conflict with goals for accessibility.

**Reliability/Availability/Maintainability**. Reliability, availability, and maintainability (RAM) concerns are caused by the vagaries of physical systems in a physical world, such as parts failure. Data networks for mission critical purposes tend to be dedicated, with limited interconnection and built in redundancy as needed, rather than relying on the redundancy of the underlying telecommunications networks.

**Manageability**. Manageability includes status, fault, configuration and performance management. While in many cases individual networks have excellent management tools for all four categories, few internetworks do. While rapid progress is being made in this area, many of the tools and techniques remain primitive. Changes in configuration, features, and security parameters can still be complex operations, and self-configuration of components remains rare.

**Useability**. The useability of a system is a measure of how easily the users of a system can accomplish their work. The level of useability has a direct impact on the life cycle cost of the system and especially on the cost of training. Factors which impact the useability of a communications mode include the human and programming interfaces, directory support, and administrative support.

**Accessibility**. Accessibility is the ability of all users, with the need and the authorization to communicate, to actually be able to communicate to fill their needs. These users may be Federal employees who need information to perform their jobs, citizens who need information about government services or need to acquire those services, industry providers of service to the government, businesses regulated by the government, or businesses requiring Federally generated information for their operations. A number of specific NPR recommendations are directly applicable to accessibility improvements. These include implementation of electronic commerce, establishment of trade and environmental data systems, and intergovernmental tax filing.

## 2.3 Affinity Groups

The Panel recognizes that government agencies have common Information Technology (IT) requirements for sharing information and would greatly benefit from having access to a Government information infrastructure. The government agencies, or functional interest groups therein, that share information electronically and have common IT requirements have become known as affinity groups. The NPR describes the affinities that exist between related government agencies. A primary benefit of identifying and fostering such affinity groups with similar requirements is that, as the common requirements of affinity group members begin to converge, the agencies can come to consensus as to how to meet the requirements in a common way. With the affinity groups identified and already working together, common solutions to internetworking requirements can be undertaken by all the agencies in the group.

To ensure that affinity group solutions also promote government-wide interoperability, there is the need for coordination across affinity groups. This coordination in turn will lead naturally to evolving convergence of views regarding the requirements for the Government information infrastructure. Because the public needs electronic access to government agency services, the Government information infrastructure should allow the public access

to government electronic services using the National Information Infrastructure (NII). For public access services, it may be important to provide a basic level of services inexpensively while a higher level of services may be available at a higher cost.

Affinity groups have a shared need or mission that can be furthered by internetworking of IT among members of the group, although IT standards and networking are not their primary focus. Affinity groups may be defined in various ways: by a common data system; by a common data requirement; by a common clientele; by the common state agencies that they interact with; or a common service delivery. They could be self-defining, or they could be established by OMB or the FIRMPoC, or by individual agencies. In addition to Federal agencies, affinity groups may possibly include state governments and the private sector.

The draft NPR Accompanying Report, titled Reengineering Through Information Technology (Office of the Vice President, 1993), includes seven recommendations for creating an electronic government based on integrated service delivery through affinity groups. Seven affinity groups are established by the NPR: integrated electronic benefit transfer; integrated electronic access to government information and services; national law enforcement/public safety network; intergovernmental tax filing, reporting, and payments processing; international trade data system; national environmental data index; and government-wide electronic mail. Three additional affinity groups are the Government research community (operating as the Federal Networking Council); the Electronic Commerce/Electronic Data Interchange (EC/EDI) working group; and Government network managers.

Because affinity groups are the context within which interoperability is important, active participation of affinity groups is required in the selection of standards (including profiles and implementation agreements) and in the development of infrastructure to support interoperability. Building on the affinity groups already established in connection with implementing the NPR recommendations, the process for identifying affinity groups, a structure for coordinating them, and their roles and responsibilities need to be defined.

### 2.4 Leading Edge and Core Services

One consequence of the rapid rate of change of network technology is that yesterday's experimental system is today's beta-test and tomorrow's production system. When Government requires deployment of leading-edge network technology, this mandates the specification of technology well before it is commonly available (for example, the specification of an experimental network).

Experimental networks are always risky and usually expensive. Hence, industry may be reluctant to deploy such networks if the risk-to-benefit ratio is too high. But if industrial and Government interests in future networking technology are aligned, Government can play an important role; by partially funding such programs - participating at the margin - it can reduce the financial risk to industrial organizations and make it attractive to them to participate. From the Government's standpoint, its investment is highly leveraged by the degree of industrial participation and a "win-win" situation results, in which industrial technology is advanced more rapidly and, at the same time, Government acquires the use of a network that is not a victim of instant obsolescence.

There is a window that, with time, slides along the technology axis of networks, in the direction of higher performance. At the leading edge of the window are found the most advanced, highly experimental networking methodologies, practiced by only a few of the most technologically aggressive companies and often as industry-Government-academic

partnerships. Standards tend to be in development and to track the changing technology. At the trailing edge of the window is the current state of commercial off-the-shelf (COTS) network technology, characterized – at least in the U.S. – by multiple private commercial suppliers, vigorous competition, and proliferation of network services offered as commodities, as competitors seek to differentiate their network offerings to achieve market share. Standards, both proprietary, as well as industry-wide, proliferate but are modified slowly, reflecting the relative maturity of the technology.

As a consumer, Government purchases core networking products and services competitively, on the open market. At the same time, Government is a partner with industry in pressing the technology forward. Agencies should distinguish between core services (e.g., electronic mail, file transfer, fax) and leading edge services (e.g., bandwidth on demand, interactive video, multimedia e-mail). Standards are important for core services which should be based on commodity products. Agencies requiring leading edge services should be able to acquire the required technology, but also be prepared to accept the risks associated with deployment prior to stable standards and commodity products.

### 2.5 Vision of Federal Internetworking

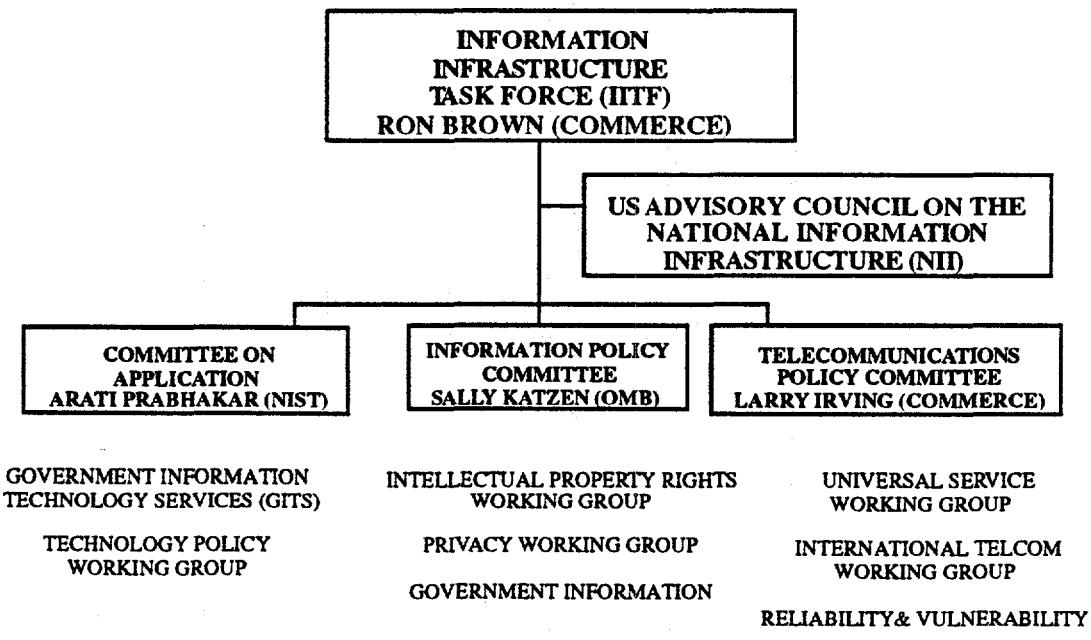
The foundation for a vision of Federal internetworking is laid out in The National Information Infrastructure (NII) Agenda for Action (Information Infrastructure Task Force, 1993) and in the draft NPR Accompanying Report, Reengineering Through Information Technology (Office of the Vice President, 1993). The vision of an electronic government requires computer hardware, software, and telecommunications equipment to make information flow smoothly across the nation's information highways. It will position the Government as a leader in IT utilization, rather than lagging behind the commercial sector, as it generally does now. It also requires policies, procedures, and standards to support the development and operations of services that use the physical technology components. An effective information infrastructure requires high levels of interpretation and integration among diverse users.

The Panel's vision is that the Government information infrastructure to support internetworking evolves as a portion of the National Information Infrastructure (NII). The Government information infrastructure must support mission needs within an agency, interoperability between agencies, and electronic access to the government from the public as well as from business and industrial partners and contractors. The Government information infrastructure should build on and integrate the current baseline which includes, but is not limited to, FTS2000 for basic intercity telecommunications, and the Internet for data communications with the public and academia. The Government information infrastructure, as a portion of the NII, must satisfy the needs of affinity groups while leveraging commercial infrastructure. The Panel envisions the Government information infrastructure as a virtual internetwork, built on the networking infrastructure primarily deployed by industry, with components supporting the specific needs of affinity groups. The Government information infrastructure will potentially require both core and leading edge services and provide access to the public through commercial, on-line information service providers, generally in the core services area.

In order to attain this vision, the Panel believes that there must be increased leadership and integration across Federal agency internetworking activities. Mandating acquisition standards is not sufficient. There must be an integrated internetworking strategy that takes into account affinity group needs, standards, infrastructure, marketplace assessment, technology maturity, and budgetary considerations. The Panel recommends that this leadership should come from OMB and the Information Infrastructure Task Force, to include an annual guidance document for Federal internetworking.

The OMB role should include those issues relating to resources, policy and oversight. Some functions could be delegated since OMB may not be positioned adequately in terms of resources and structure. OMB responsibilities include budget review and support of incentives for agency initiatives that contribute to improved Federal internetworking. OMB should provide guidance to ensure monetary resources are available to carry out the plans and infrastructure in accordance with a coordinated government-wide strategy.
The Panel believes that the annual document is key to providing a single, integrated internetworking strategy both within Government and to the public. Specific areas to be addressed in this include: the current assignment of Federal internetworking requirements to specific networks, i.e., advanced research and development, leading edge or core/commodity services; transition strategies; relevant policy (e.g., interface requirements, acquisition guidance, budgetary guidance, etc.); and a market assessment.

The White House formed the Information Infrastructure Task Force (IITF) to articulate and implement the Administration's vision for the National Information Infrastructure (NII). The task force consists of high-level representatives of the Federal agencies that play a major role in the development and application of information and telecommunications technologies. The task force operates under the aegis of the White House Office of Science and Technology Policy and the National Economic Council. Three IITF Committees have been established: Telecommunications Policy, Information Policy, and Applications and Technology. The committees and the working groups within them are illustrated in the accompanying figure. The Government Information Technology Services (GITS) working group coordinates efforts to improve the application of information technology by Federal agencies. It is responsible for implementation of the recommendations in the National Performance Review draft Accompanying Report, titled Reengineering Through Information Technology, and for coordinating these initiatives with initiatives involving the NII.




A common vision as to how the Federal Government should be interconnected within itself and with the public is paramount. This common vision should embrace not only the underlying networking facilities but also the more application-oriented services required to

access information and conduct commerce as a portion of the NII. This area is primarily a responsibility of the GITS working group. An effective strategy would start with the development of functional requirements and a conceptual architecture for access to government information and services on the Government information infrastructure. The IITF, primarily through the GITS working group and in collaboration with state and local government and the private sector, should begin by developing a Government information infrastructure concept that will link requirements and goals with technical options and opportunities for service delivery; identify key factors that need attention; and address such issues as user-friendliness, standards, cost, and inter-government cooperation. Such a concept would primarily address integrated electronic access to Government information and services as a seamless part of the NII.

## 2.6 Summary and Conclusions

Although the Panel focused primarily on requirements for data internetworking, it recognizes that the trend is for data to be one component of multimedia information that may include voice, video, and image components. As the recommendations of the NPR begin to be implemented, there will be increased demands for interoperability between Government agencies as well as between Government and the public, as an essential part of every agency's mission. Affinity groups, Government agencies that have common requirements for sharing information, have come into existence as a result of the NPR. Some affinity groups focus on Government wide topics, such as electronic mail, while others focus on specific applications areas.

With the rapid rate of change of network technology, a distinction needs to be made between core/commodity services, leading edge services, and advanced research and development. Standards are particularly important for core services that should be based on commodity products. Agencies requiring leading edge services should be able to acquire the required technology, but also accept the risks associated with deployment prior to stable standards and commodity products.

The Panel's vision is that the Government information infrastructure evolves as a portion of the National Information Infrastructure (NII). In order to attain this vision, there must be increased leadership and integration across Federal agency internetworking activities. There must be an integrated internetworking strategy that takes into account affinity group needs, standards, infrastructure, marketplace assessment, technology maturity, and budgetary considerations. This leadership should come from OMB and the IITF.

## 3.0 INTERNATIONAL INTEROPERABILITY AND TRADE

Federal agencies have requirements for international interoperability with other nations that are usually satisfied by the use of voluntary international standards and the international public infrastructure. In addition, products and services to satisfy agencies' internetworking needs are obtained from the international commercial open market. There are international inter-relationships between standards, public infrastructure, obligations, the marketplace, and trade and national competitiveness.

### 3.1 Formal International Standards

Formal international standards such as those from ITU and ISO, are agreed to according to due process and established procedures, and they have the formal recognition of governments worldwide. To gain the approval of governments, most voluntary standards organizations either seek the formal route of obtaining peer-to-peer liaison status with the widely recognized international standards organizations, or they submit their standards through existing third party routes such as through a national body (e.g., IEEE LAN standards take this route) or through another liaison organization. The subject of Internet Society liaison to ISO/IEC Joint Technical Committee 1 (JTC1), as well as the general subject of JTC1 recognition and utilization of standards developed by non-ISO/ITU bodies, is currently under active discussion within JTC1. See also Section 4.3.

### 3.2 International Public Infrastructure

In providing for international interoperability, the international public communications infrastructure offers the most leverage. Simply by virtue of market pragmatics, any user who is connected to the worldwide public networks through commercial off-the-shelf hardware and software systems has a practical basis for a degree of interoperability with other users. Two users who interconnect to the worldwide X.25 network, the worldwide telephone network, or the worldwide Internet, have a degree of interoperability based on their end-systems hardware and software interfaces and protocols. X.25 and X.400 services are available from public carriers almost worldwide and are important for international business communications. Agencies should be able to establish international interoperability across any of these networks that meet their needs.

For newer technology networks, such as Integrated Services Digital Network (ISDN), Frame Relay, Synchronous Digital Hierarchy (SDH), Broadband ISDN (BISDN) or Asynchronous Transfer Mode (ATM), the end-to-end interconnectivity and infrastructure is not currently as well established as the older networks, but instead, is a matter of intense interoperability agreement development in Committee T1 in the U.S., in the ITU, and in user groups such as the North American ISDN Users' Forum (NIUF). The Federal Government should participate in these groups as needed to assess their potential for meeting their needs and for achieving international interoperability. Until the international interoperability is established and the international infrastructure is in place, use of these newer technologies to meet agency mission needs will have to be balanced against risk, cost, and the effects of limited availability.

Perhaps the dominant international data interoperability user group is the Internet community. It has international scope for its open process of developing and promoting Internet drafts, proposed standards, and recommended standards, and of fielding public domain interoperable implementations. Moreover, Internet standards and even proposed standards are often quickly available internationally as services on the Internet (e.g., the rapid growth of Gopher, Wide Area Information Servers (WAIS), and World Wide Web, or the rapid deployment of IP multicasting in the Multicast Backbone (MBone)). Agencies

should have the freedom to select the IPS for international interoperability with other agencies by connecting to the international Internet infrastructure when it meets their needs and by acquiring products based on these interoperable implementations.

### 3.3 Multinational Commercial Products

Another widely used approach for achieving international interoperability is to exploit the increasingly multinational commercial character of the computer and communications marketplace. Multinational consortia such as X/Open, ATM Forum, and Open Software Foundation (OSF) are increasingly becoming responsible for defining and promoting internationally interoperable enterprise solutions. Consortia (discussed more fully under Standards Process) frequently can develop quick, industry-wide consensus for emerging technologies. The consortium approach needs to be recognized as an acceptable process when aimed properly at promoting the rapid development of open products from multiple vendors and the rapid deployment of international infrastructure. Governments and large users should be vigilant to join consortia as appropriate to keep them focused on open global market building to meet user needs and keep them from degenerating into noninteroperable market islands or regional differences.

Proprietary but highly popular product implementations, such as Postscript and WordPerfect have become the "common-use standard" for many commercial organizations. Governments should also be able to buy these products when "international standard" solutions are not widely available in the marketplace.

Open markets provide the highest quality, most cost-effective multivendor international interoperability, as long as buyers hold the vendors accountable for their claims. Well known multinational vendors such as Sun, HP, DEC, IBM, Novell, Microsoft, Intel, Cisco, 3Com, Synoptics, and many more, have products that have acquired significant market share because of their functionality, cost effectiveness, and open interfaces.

### 3.4 International Obligations

The ITU is a formal treaty organization, organized and run under the auspices of the United Nations. The ITU Telecommunication Standardization Sector (ITU-T) produces Recommendations, some of which are endorsed as standards by member countries. The United States is represented in the ITU by the Department of State which is the X.400 Administration in the U. S. Global addressing schemes, defined and allocated by ISO and ITU-T, are accepted by carriers and governments worldwide.

In NATO, the overall strategy for improving interoperability of data systems is based on the use of civil international standards to the maximum extent possible, i.e., on OSI. Now being developed, the NATO Open Systems Interconnection Profile (NOSIP) is patterned after national GOSIP programs, to facilitate the identification, specification, acceptance and procurement of military communications and information systems. NOSIP describes internetworking approaches based on both connection-oriented and connectionless mode network services. NATO infrastructure policy permits use of TCP/IP. With the growth of LAN complexes at NATO sites and the need to interconnect these sites, there is an ever expanding use of IP router implementations. Within NATO, interoperability experiments/developments dealing with OSI applications like X.400 and X.500 use TCP/IP to provide the underlying transport service.

The Federal Government is using both OSI and IPS to satisfy international communications requirements. Major research agencies such as NSF, ARPA, DoE, and NASA, make extensive use of the Internet in support of worldwide scientific research and collaboration.

NASA, NOAA, and DoE have extensive requirements for worldwide exchange of earth observation and environmental information with their counterpart agencies in other countries. Some Internet links between the U.S. and foreign networks are for mission-specific purposes, while others are part of the infrastructure or are provided under cooperative agreements with carriers. The Internet and the IPS are pervasive in the international research community, with OSI use limited to X.400, X.500, and a Connectionless Network Service (CLNS) pilot. However, some agencies also use OSI and proprietary protocols as the core of their international communication networks.

The global air transport community is migrating to OSI. The Aeronautical Telecommunications Network (ATN), based on OSI, is designed to facilitate communications between aircraft and ground-based airline and air traffic control systems. The FAA has actively participated in the development and implementation of these systems and has a major stake in OSI.

Many other governments have adopted policies similar to the current U.S. GOSIP (e.g., U.K., Europe, Australia, Canada, New Zealand). These governments have harmonized their policies and procurement profiles through the International Public Sector Information Technology (IPSIT) group, in which the U.S. is represented by NIST. Proposed changes to U.S. GOSIP policy should also be advocated within this group, to benefit the government information technology (IT) activities of all countries involved. Other IPSIT members are generally still committed to OSI as the single long-term solution, although some have a more explicit acceptance of TCP/IP as an interim solution. It is not known to what extent this commitment to OSI by the standards-oriented bodies is shared by network user agencies in those countries. Some IPSIT members (Australia, Sweden) appear willing to accept IPS protocols alongside OSI.

### 3.5 International Trade and National Competitiveness

The U.S. Government fosters international free trade as a matter of public policy, to allow U.S. industries to compete effectively on an internationally level playing field. U.S. buyers are best served when they can choose freely among the highest quality and best value products available in the open world marketplace. However, achieving agency international interoperability may involve some difficult international trade issues.

The Office of U.S. Trade Representative (USTR) is responsible for obtaining, through bilateral and multilateral negotiations, such as the General Agreement on Tariffs and Trade, the most level playing field possible for U.S. products including computer and communications products. The USTR is able to use the market success of U.S.-based multinational computer and communications companies as an example of the benefits of free trade. Agencies will then have to abide by the agreements negotiated by the USTR such as agreements that require some uniformity in the use of international standards to qualify products so as to eliminate nontariff barriers to trade.

The North American Free Trade Agreement (NAFTA) calls for efforts to make standards developed by recognized standards bodies compatible between Mexico, Canada, and the U.S. The objective in NAFTA is to promote trade and interoperability. Alignment between national voluntary and consortia standards is important to facilitate the NAFTA objectives and process.

U.S.-based multinational companies in the computer and communications fields are aggressively seeking to expand their worldwide market shares. U.S. agencies should be able to take advantage of and assist this national competitiveness by acquiring products and services that promote U.S.-based multinational solutions. Foreign companies are also

searching for ways to lead the marketplace. If U.S. internetworking technologies have a prominent role in the international interoperability solution marketplace, then it is advantageous for U.S. agencies to use these same solutions to interconnect with domestic and international partner agencies, thus further growing the market. Agencies should be allowed to use the best available international open solutions to achieve their mission interoperability needs, also based on quality and value in the competitive marketplace.

As far as the Panel has been able to determine, if the U.S. Government makes other open voluntary international standard protocols co-equal with OSI protocols, this would not violate any treaty obligations. In the European Union, procurers have to refer to ISO standards, so IPS protocols could encounter difficulty in acceptance there without recognition by ISO unless similar policies are adopted to those being proposed for the U.S.

### 3.6 Summary and Conclusions

The international public infrastructure, including the worldwide telephone network and carrier-provided data networks, are based on formal international standards. Global addressing schemes, defined and allocated by ISO and ITU-T, are accepted by carriers and governments worldwide. The Internet also provides worldwide connectivity.

Many Federal agencies have requirements for international interoperability. Some Federal agencies have a major commitment to international systems based on OSI (e.g., FAA), while other agencies could not meet their mission needs without the IPS and the Internet (e.g., NSF, NASA). Agencies and interagency coordinating committees (i.e., affinity groups) should work with their counterparts in other countries to establish worldwide interoperable solutions between partner government agencies, as appropriate to meet their mission needs. The multinational computer and communications product marketplace and the international public infrastructure should have an equal place alongside the international standards for providing legitimate means for agencies to achieve their interoperability goals.

While there do not appear to be any treaty obligations that restrict the U.S. Government from selecting other non-ISO open voluntary international standard protocols, the Panel understands that other governments may require the use of ISO standards. Proposed changes to U.S. GOSIP policy should be advocated by NIST within the International Public Sector IT group (IPSIT), to describe the U.S. recommended approach clearly and to explain its rationale and benefits.

# 4.0 STANDARDS PROCESS

## 4.1 Goals of Standards

Standards by themselves are not a goal but are a means for achieving goals. Standards should facilitate the following goals for Federal internetworking.

**Fulfilling Federal Mission Needs.** Satisfying agency mission needs is the highest priority of Federal internetworking. For example, the NPR identifies seven needs for electronic government networking, including integrated electronic access to government information and services and a national law enforcement and public safety network.

**Enabling Interoperability.** The coming electronic government and electronic society requires that government agency systems have built-in interoperability, independent of specific mission need. For example, the NPR identifies the need for government-wide electronic mail. Interoperability of government and private sector systems is key to providing service to the citizen.

**Providing For Software And Hardware Portability.** Portability enables software and hardware developed in one environment to be applied easily in other environments for other uses. Software and hardware portability reduces the time, effort, and cost needed to apply existing solutions to new problems.

**Lowering Cost.** Standards-based solutions which are widely applicable are almost always lower in cost because of competition and volume. Solutions bought in large numbers provide an attractive marketplace, resulting in effective competition. Standards-based products which are widely available in the marketplace are good for everybody: users, vendors, and taxpayers, since they result in both lower acquisition and life-cycle maintenance costs.

## 4.2 Development and Use of Standards

Standards specify the network interfaces and the dynamic interactions ("protocols") between heterogeneous systems. However, there are many standards developing organizations. In this section, background information is provided on the types of standards organizations. More comprehensive information on this topic may be found in (Cargill, 1989).

The highest level of international acceptance is usually associated with international standards that have been approved by the formally recognized international standards bodies. These are the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunication Union (ITU). The OSI standards have been approved by the ISO/IEC Joint Technical Committee 1 (JTC1) and/or the ITU Telecommunication Standardization Sector (ITU-T).

In the U.S., national standards are usually developed by voluntary standards developing organizations accredited by the American National Standards Institute (ANSI). Examples are the Accredited Standards Committee (ASC) for Information Processing Systems (X3), the ASC for Telecommunications (T1), and the Institute of Electrical and Electronic Engineers (IEEE). National standards are often superseded by, or aligned with, international standards. In other cases, national standards may be a specific subset or set of options within an international standard.

In recent years, there has been a proliferation of a wide range of new standards developing organizations in the information technology field that are usually described in the category of consortia. A major motivation for some of these organizations has been the rapid pace of technology development compared to the relatively slow pace of the formal national and international standards organizations. Some consortia exist to refine and build on the formal international standards by defining subsets or sets of options so as to ensure interoperable implementations between vendors. Examples of this latter type are the Open Systems Environments Implementors Workshop (OIW) and the ATM Forum.

De facto industry standards are based on proprietary protocols, although in some cases the specifications are publicly available and widely accepted and adopted by many suppliers. Publicly available specifications allow an open market to exist and interface to a proprietary product. However, they are not controlled by a standards organization or independent consortia. Examples are MS-DOS, Microsoft Windows, and Adobe PostScript.

### 4.3 The Internet Standards Process

The Internet standards process is of particular concern because of the widespread impact of the IPS on the marketplace, yet the IETF is operating outside the traditional standards structure. Standardization of the IPS is carried out by the Internet Engineering Task Force (IETF). The IETF is managed by the Internet Engineering Steering Group (IESG) whose operation is overseen by the Internet Architecture Board (IAB) and whose procedures are approved by the Internet Society (ISOC). The current Internet standards process is defined in RFC 1602 (IAB and IESG, 1994).

The IETF is not formally accredited as a standards developing organization. Although the IETF fulfills some of the requirements of such organizations, such as having written procedures that provide for due process and openness, the IETF does not practice formal voting as a means of assuring consensus and balance. The ISOC is not formally recognized by ANSI or ISO, although discussions with JTC1 have been going on during the past year and JTC1 has approved Category A liaison between SC 6 and ISOC. On the other hand, the Internet standards process is contributing substantially to the goals of internetworking by producing standards many of which are widely supported in the marketplace. Moreover, the IETF philosophy of "rough consensus and running code," which emphasizes multiple implementations and experimentation in parallel with standards specification development, has resulted in products reaching the marketplace more quickly compared to OSI.

The formal standards process has not produced convergence but has resulted in multiple standards for equivalent functions, a situation which led to the creation of this Panel. However, the fundamental issue is not the relative technical merits of various OSI and IPS protocols, but the existence of two different standards processes, one traditional and formal, the other new and with substantial positive influence on the marketplace.

The IPS is widely accepted in the marketplace as a source of standards to support internetworking. The Panel believes that standards should be judged by the products they produce in international markets. On this basis, as far as the U.S. Government is concerned, the Panel believes that IPS standards should be treated the same as any other open, international, voluntary standards. Protocols from IPS should be accepted as co-equal with protocols from the OSI suite.

There are some areas, such as standards for addressing schemes and administration over allocation of addresses, for which it is extremely important to have a single standard and process to provide worldwide connectivity. The international community and other

governments will only accept formally recognized international and national organizations dealing with such matters. The long term goal of harmonizing on a single standard for each function, and the interests of vendors and users, would be better served if the JTC1, ITU-T, and IETF would agree on a mechanism for recognizing the IETF's technical work. Thus, while accepting and using appropriate IPS standards as discussed in the following section, the U.S. Government and its representatives should use all their influence with the various standards bodies to work towards convergence and harmonization of the standards process.

### 4.4 Federal Internetworking Standards Selection

**GOSIP Objectives.** The essential goals of GOSIP are unchanged, but the means of achieving them need to be changed if the intent of GOSIP - to promote network interoperability - is to be realized. The primary objective of GOSIP is "To achieve interconnection and interoperability of computers and systems that are acquired from different manufacturers in an open systems environment." (NIST, 1991) This is still the key overall objective of Federal internetworking. Two other objectives of GOSIP are unchanged: "To reduce the costs of computer network systems by increasing alternative sources of supply;" and "to facilitate the use of advanced technology by the Federal Government." The fourth and final objective of GOSIP, which refers specifically to OSI standards, should be modified to reflect the wider range of standards in the marketplace. The Panel believes that the special exclusive status of the OSI standards as the only recognized international standards should be removed, and such status extended to the IPS as well as OSI. In addition, the name of GOSIP should be modified to connote selection from a broader range of allowable internetworking protocols, e.g., Government Open Systems Profile (GOSP), Government Profile for InterNetworking (GPIN), or Profiles for Open Systems Internetworking Technologies (POSIT).

**OMB Circular A-119.** OMB Circular A-119, revised, October, 1993, "Federal Participation in the Development and Use of Voluntary Standards," (OMB, 1993) provides Federal policy guidance in this area. Voluntary standards bodies are defined as private sector domestic or international organizations that plan, develop, establish, or coordinate voluntary standards. The circular states that, when properly conducted, standards development can increase productivity and efficiency in Government and industry, and expand opportunities for international trade. A-119 states that voluntary standards are preferred for Federal use, and that international standards should be considered in the interests of promoting trade. At the end of the circular, a letter from the U.S. Department of Justice, Antitrust Division, states that "the potential for anticompetitive harm resulting from industry standards setting can be reduced to the extent that such proceedings are open and transparent and provide an opportunity for notice and comment to any person potentially affected by the promulgation of the proposed standards." The circular does not mention the concept of "accreditation". The Panel believes that the use of IPS standards is consistent with A-119.

**Selection Criteria.** The Panel believes that the selection of standards for Federal internetworking use should be influenced by several factors: technical, marketplace, and status as a standard. Technical considerations include:

- meeting government needs
- necessity for interoperability
- compatibility with long-term vision
- compatibility with existing infrastructure
- transition costs for legacy systems.

The maximum attainment of the goals of GOSIP requires the use of standards-based solutions characterized by the following marketplace criteria:

- actually working
- in widespread use
- implemented on multiple platforms
- openly specified
- provided by multiple sources with viable competition.

The status of the standard is yet another factor to be considered. International standards are desirable, other factors being close to equal, to facilitate international interoperability and in the interests of promoting trade. Other types of standards, in order of preference when other factors are close to equal, are national standards, consortia standards, and de facto standards based on proprietary protocols. Proprietary protocols are only selected as a last resort when no other types of standards meet the marketplace and other criteria. This may be for leading edge technologies, or to meet the needs of an affinity group. The necessity to use a proprietary protocol is an indication of an area where standards work is to be encouraged. Federal preferred standards should be selected taking into account the technical, marketplace, and standards-status factors discussed above. The original GOSIP policy focused only on OSI candidates, in the expectation that they would come to dominate the market and satisfy the other factors. However, it is clear that protocols in both the OSI and IPS satisfy many of the above factors, and that neither stack alone meets the Government's needs. Thus, appropriate standards should be drawn from both OSI and the IPS and possibly other sources. While a single standard for each function would be the ideal and remains the long-term goal, the reality is that in the near-term, for some functions equivalent protocols from both stacks may be included in a Government networking profile, based on government needs and their technical and marketplace strengths. The Government Network Management Profile (GNMP), FIPS 179, as currently defined, does not reflect the above criteria for the selection of standards.

**Scope of GOSIP.** The current GOSIP includes everything from physical layer to application layer, with several options at some of the layers. A common standard at certain layers is important to attaining end-to-end connectivity and interoperability. However, subnetworks employing different technologies at the lower layers (physical and data link) can be interconnected through a common internetworking protocol at the network layer. Several LAN protocols, X.25, and ISDN are currently included in GOSIP; however, there are several newer technologies such as FDDI, 100 Mbps Ethernet, Frame Relay, and ATM which are not currently in GOSIP. There is no need to mandate specific technologies at these lower layers to attain connectivity, and in view of the rapidly evolving marketplace, users should be free to select according to their needs and marketplace considerations. The important thing is a common interface to subnetwork technologies, such as the logical link control sublayer (ISO 8802), or use of IP over Frame Relay or ATM.

It is most important to have common standards at the network and transport layer, to provide basic connectivity including addressing and routing. Common standards for applications are desirable to facilitate end-to-end interoperability, and although corresponding standards can interoperate through gateways (such as X.400 to SMTP), there is usually some loss of functionality. The scope of GOSIP should be limited to these applications that are needed for core government-wide services and for government interoperability with the public. These include electronic mail/messaging, file transfer, directory access, EDI, and security including digital signature. The additional standards needed for a specific application (such as benefits transfer or medical records) should not be part of GOSIP but should be the responsibility of the appropriate affinity group, potentially in conjunction with industry and appropriate voluntary standards bodies.

**Applicability of GOSIP.** The applicability statement in GOSIP currently states that "GOSIP shall be used by Federal Government agencies when acquiring computer networking products and services and communications systems or services that provide equivalent functionality to the protocols defined in the GOSIP." The policy permits agencies to buy network products in addition to those specified in GOSIP, including other non-proprietary protocols, proprietary protocols, and features and options of OSI protocols which are not included in GOSIP. Although agency heads may approve waivers, they must provide a written explanation of the basis for the decision to NIST, with notification to appropriate committees of the House of Representatives and the Senate. Few, if any, waivers have been approved, and instead agencies have complied by acquiring GOSIP protocols even if they are not used.

The Panel believes that the protocols in a broadened GOSIP should be mandatory for consideration for use. Large communications systems are rarely acquired from scratch but tend to evolve, and the past focus on procurement had little influence on actual operation and use. Consequently, the policy should focus on using, or planning for transitioning to use, one or more of the protocols specified for a given functionality that is needed. The process should recognize that no predetermined set of standards will fit all situations, and that when this is found to be the case after real consideration, appropriate decisions can be made on a case by case basis. A simple certification by the requisitioner saying that the required consideration had been given would suffice. The policy should also clarify whether one or more of the protocols specified in the broadened GOSIP are required in every component of a system with that functionality (such as a personal computer), or whether the essential interoperability can be satisfied by a gateway to the specified protocol. For example, is standard e-mail (such as X.400 or SMTP) required on every desktop, or can some proprietary e-mail system be used locally so long as there is a gateway to the required standard. It is suggested that the gateway interface is the minimum required, and the choice of required protocols in every component can be weighed against the functionality, other benefits and costs.

**Convergence.** The inclusion of protocols from both the IPS and OSI in a broadened GOSIP inevitably raises the issue of interoperability between communities using different protocols, and strategies for convergence to a single solution. The Panel believes that the long-term resolution lies in harmonization of the standards process, as discussed in section 4.3. In the near and mid-term, coexistence and interoperability are inevitable and practical, although imperfect. Commercial routers support IP, CLNP, and proprietary protocols, enabling coexistence of different protocols on a shared backbone without interoperability. The Internet carries both IPS and OSI applications, using RFC 1006 for OSI applications over TCP/IP. X.400 to SMTP mail gateways provide interoperability, albeit with lowest common denominator functionality.

There are two areas where the Panel believes immediate attention is warranted to start to bring the existing IPS and OSI stacks together: the network layer, and the transport layer interface. A new internetworking protocol is required by the Internet because of address space limitations. The IETF has been working for some time now on the specification of a new Internetworking layer, to transition to from the existing IPv4. This process is based on trying to achieve compatibility with the existing base of deployed network and host hardware and software, the ability to scale to very large sizes, and to add new functionality in the areas of resource control, management and security. The Panel believes that the convergence of both IPS and OSI to this new internetworking layer would be a win-win situation for all groups. A single standard recognized by both the IETF and JTC1 would have far wider acceptance than CLNP, and would promote the harmonization of upper

layer protocols between the groups. A single naming and addressing scheme that is accepted worldwide is essential for international interoperability.

The path to convergence is for OSI and IPS applications to coexist over a common transport and internetworking protocol. RFC 1006 was originally created to foster a testing atmosphere for OSI protocols (Transport and up) over the existing Internet. RFC 1006 specifies Transport Class 0 over a TCP socket. However, RFC 1006 has some weaknesses (overhead and behavior problems) and there are other different non-interoperable variations for implementing OSI over TCP/IP. There is now a strong requirement for standardization of hybrid solutions, such as a stack for interoperable use of X.400 over TCP/IP.

The Panel recommends that the IETF and JTC1 SC 6 jointly establish convergence workshops that take advantage of the best characteristics of both organizations, to focus on the above and other convergence issues that may be identified. The technical output of the workshops would be processed by both organizations. The Government through its representatives and members should urge both standards organizations to collaborate on these immediate technical areas while continuing discussions on the long-term harmonization of the standards process.

### 4.5 Testing

Product conformance and interoperability is a major consideration. Adopting standards always involves the consideration of how to test that delivered products conform to the standards and that products from different vendors interoperate. The current GOSIP policy emphasizes conformance testing, and requires that products be qualified before procurement by an accredited testing laboratory when a test capability is available. GOSIP version 2 recommends interoperability testing and states what must be specified. The GOSIP conformance testing process, while rigorous, is very expensive to develop and execute definitively with rapidly evolving and integrated products. This has contributed to the delayed availability and cost of GOSIP products. In contrast, the Internet requires at least two independent implementations and interoperability testing before approving an Internet Standard, and therefore is cheaper and faster because of the close interaction between standardization and product development.

The Panel believes that the Government, as a user of information technology, and not a developer of such, is primarily concerned with the interoperability and robustness of internetworking products, and not their conformance to a specific standard. This is consistent with maintaining the focus on the results of successful standards use, and not a focus on standards by themselves. Therefore, from the Government's perspective, conformance testing is not an end in itself, and is primarily a vendor responsibility. Vendors need to commit to the quality, features and interoperability of their products on an ongoing basis. Written warranties are an appropriate method for vendors to demonstrate their commitments. The Government should suggest standard wording for warranties which would encourage a pricing structure based on quality, features and interoperability of services and products. Having a limited range of interoperability testing options available would permit agencies to choose the degree of confidence they need relative to cost, to account for the differing mission-related requirements of various agencies. Less testing is needed for commodity products with widespread deployment. The Government should require their own interoperability tests for high assurance systems.

Interoperability testing may consist of testing against a reference implementation or multivendor interoperability testing. Reference implementations may be developed in conjunction with the standards development process. Multivendor interoperability testing

groups may be formed by vendors, sponsored by a standards organization, or sponsored by an independent organization. Examples are the FDDI interoperability test lab at the University of New Hampshire, and the OSPF interoperability group. Agencies should encourage vendors to participate in such testing groups, and may wish to participate directly themselves, to ensure the testing done is aligned with their requirements for product interoperability.

It is important that both kinds of testing should be harmonized internationally with European and Asian efforts. NIST should collaborate with fellow IPSIT members on the international harmonization of the warranty of products.

### 4.6 Summary and Conclusions

The fundamental issue is not the relative technical merits of various OSI and IPS protocols, but the existence of two different standards processes. The long-term goal of harmonizing on a single standard for each function would be better served if the JTC1, ITU-T, and IETF would agree on a mechanism for progressing the IETF's technical work into other related international standards bodies.

The essential goals of GOSIP are unchanged, but the means of achieving them need to be changed if the intent of GOSIP is to be realized. GOSIP should be broadened since no one stack meets the Government's needs, and to reflect the wider range of open networking standards-based products in the marketplace. The selection of protocols for a broadened GOSIP should be based on technical and marketplace factors and status as a standard with appropriate standards drawn from both OSI and IPS and other viable sources.

The scope of GOSIP should be limited to the network and transport layer, the interface to the logical link control sublayer, and those applications needed for core government-wide services and for government interoperability with the public.

The applicability statement in GOSIP should be modified such that the protocols in a broadened GOSIP are mandatory for consideration for use.

JTC1 and the IETF are urged to jointly establish convergence workshops to develop technical solutions to the interoperability issues resulting from the acceptance of protocols from both OSI and IPS. Two areas where immediate attention is warranted are the transition and convergence of IP and CLNP, and an updating of RFC 1006.

The Government is primarily concerned with the interoperability and robustness of internetworking products. Conformance testing should be primarily a vendor responsibility to warranty their products. A limited range of interoperability testing options would permit users to choose the degree of confidence they need relative to cost. NIST should collaborate with fellow IPSIT members on the international harmonization of the warranty of products.

## 5.0 TECHNICAL ISSUES

### 5.1 Functional Comparison of IPS and OSI

A document prepared by NIST provides a comparison of the functionality of the IPS and the OSI protocol suite (NIST, 1993). That document identifies technical differences between the two suites while emphasizing that in many cases, the two suites can be viewed as complementary. The Panel accepts that document as an even-handed assessment of the two suites. The following is a summary of the NIST report.

**Lower Layers.** In the case of the lower layers (network and transport), there are many similarities between the two suites as a result of cross-fertilization in their development. The OSI internet protocol, CLNP, and transport protocols drew heavily from the design and experiences of the IPS Internet Protocol (IP) and Transmission Control Protocol (TCP). The design of recent routing protocols in both the IPS and OSI suites have been influenced by each other. The IETF is currently dealing with the routing and addressing problem in the Internet. IP is running out of address space as a result of the tremendous growth of the Internet combined with the limitations of the 32 bit IP address. There is an explosion of routing information because IP network numbers are treated as flat identifiers for the purpose of routing. This flat numbering is being addressed by the current worldwide deployment of Classless InterDomain Routing (CIDR) technology, and address allocation, which should greatly alleviate the routing problem, which is the only real problem in the short-term. The address space problem needs to be dealt with, but is a moderate term problem, not a short term one. The IPS will have to evolve to a new internetworking protocol (almost certainly the result of the IETF's IPng activities) that will deal with the mid-term problem of address space, and preserve the scalability of the CIDR approach. In contrast, the OSI internetworking protocol (CLNP) does not have an address space problem, per se, but it is unclear whether or not the existing recognized allocation plans for the use of the CLNP address space would be able to scale to the size being targeted for IPng.

Almost all vendors of host computers, networking components, and distributed applications software offer support of IPS protocols. Most large vendor's multi-protocol routers also support CLNP and its associated routing protocols (with the exception of the Inter-Domain Routing Protocol (IDRP), due to its recent emergence). Many computer system vendors support TP4/CLNP lower layers as extra cost options, although support by LAN operating systems is less widespread. The biggest difference between the two suites at the lower layers is in operational deployment and experience. The extent of IPS deployment is measured not only by the size of the Internet, but also by IPS deployment in private networks that are not part of the Internet. In contrast, there is no comparable OSI infrastructure; although major backbone networks of the Internet offer CLNP switching services, these are lightly used. The number of personnel experienced in the management and administration of IPS networks relative to OSI networks is proportional to the relative size of their respective installed bases.

**Electronic Mail.** In the case of upper-layer services and applications, the OSI standards define a richer set of functionality in some cases. The IPS electronic mail application, Simple Mail Transfer Protocol (SMTP), contains many services similar to the OSI X.400 message handling system. A service included in X.400 which is not present in SMTP is standardized acknowledgments. The Multi-media Internet Mail Extensions (MIME) to SMTP expand the message format to include non-ASCII text and multi-media attachments. X.400 interpersonal messages may contain multiple body parts such as text, fax, voice, word processing documents, and spreadsheets. In addition, X.400 can be used to convey electronic data interchange (EDI) messages for business applications between computer

applications. Proprietary electronic mail systems are widespread, with SMTP or X.400 gateways used to provide external interoperability, but the additional X.400 or MIME functionality is seldom made available to users.

**Network Management.** The network management application services in the IPS are collectively referred to as the Simple Network Management Protocol (SNMP). The corresponding set of services in the OSI suite are collectively referred to as the Common Management Information Protocol (CMIP). Both the IPS and OSI management models utilize a client/server model, where the server contains managed resources and the client requests services from the resources. The IPS management protocol has had widespread implementation by many vendors over the last several years. The OSI management protocol has been slow to be deployed. Recent work has focused on interworking of the IPS and OSI management protocols. Currently, SNMP seems to be the protocol of choice for managing multi-protocol networks.

**File Transfer.** The IPS file transfer application, the File Transfer Protocol (FTP), is a simple protocol designed to transfer files between remote hosts. The OSI counterpart, File Transfer, Access and Management Protocol (FTAM), is more sophisticated with additional capabilities such as the ability to access, manipulate, and transfer portions of an entire file. Commercial implementations of FTP are widely available and FTP is widely deployed throughout the Internet. The provision and use of anonymous FTP services is the primary mechanism for the public sharing of files in the Internet community. Commercial FTAM implementations are also available for most computing environments, although most current FTAM products only implement the simple file transfer and management profiles.

**Remote Login (Virtual Terminal).** The IPS virtual terminal protocol, TELNET, was designed with scroll mode terminals in mind, although some page mode terminal properties can be negotiated. The OSI Virtual Terminal (VT) application provides mechanisms to insulate application processes from the specific characteristics of the terminals with which they communicate. The VT standard and implementors' groups have defined several profiles for specific types of terminals and applications, including the Generalized TELNET profile to support services equivalent to those provided by the IPS TELNET, the Forms profile to support the use of forms-based, field-oriented, data-entry applications, and the Paged Application profile to reflect the functionality of existing block-mode terminals. IPS TELNET implementations are widely available and used extensively on the Internet for remote login. Users can procure VT implementations supporting several asynchronous mode profiles, but actual deployments of VT are not widespread today.

**Directory Services.** In the IPS environment, there is no integrated directory service, but look-up capabilities are provided by three components: WHOIS, the Host Table, and the Domain Name System (DNS). WHOIS is a database service that can be queried for information about network users, Internet host machines, and the hierarchical domains used for naming purposes within the Domain Name System. The Host Table contains the official name and network address of network components that may be queried or copied. The DNS is a hierarchical distributed database system with servers that provide translation between host name and corresponding host address, and vice-versa. The OSI directory, commonly referred to as X.500, is designed to be a highly scalable and extensible distributed database system. The OSI Directory has many standardized object classes including people, organizations, organizational units, countries, localities, and application processes. The architecture of the OSI Directory is specifically designed to accommodate a broad spectrum of locally defined objects and attributes without the need to modify either the standard or server implementations. WHOIS and DNS are widely used by the IPS community; the Host Table is used by legacy implementations that have not been converted to use DNS. The OSI X.500 Directory is being deployed in a large number of countries,

including a large-scale pilot in the U.S. and deployments in Europe that contain over one million user entries. In most of these deployments, the OSI Directory is used in conjunction with RFC 1006 which specifies a mechanism that allows OSI applications to run in the IPS environment.

The above summary comparison covers the most basic services. Additional areas of comparison exist, for example, security services to be addressed in the next section. Moreover, there are areas where no direct comparison is possible because a capability exists in only one suite. Some examples are discussed in section 5.3. The bottom line is that both the IPS and OSI suites have desirable features that satisfy some requirements.

### 5.2 Security

This section summarizes and expands upon the comparison contained in the NIST report for IPS and OSI security. As with the other areas, the situations are not directly comparable, because the Internet situation involves both a protocol suite and an extremely large operational system. A distinction can be made between three kinds of security capabilities: design in protocols and standards; implementation in products; and operation and deployment. The Internet community has worked mostly bottom-up, focusing on concrete implementation and deployment of individual protocols designed for specific purposes, with little emphasis on security. The OSI community has worked top-down, concentrating on abstract models and architectures, including a security architecture and security frameworks.

At the lower layers, the Secure Data Network System (SDNS) has formed the basis for defining security protocols in both the OSI and IPS suites. The OSI Network Layer Security Protocol (NLSP) and Transport Layer Security Protocol (TLSP) are now International Standards. Equivalent work in IPS lower layer security is in its early stages. Security features were introduced with the 1988 version of X.400, but have not been widely implemented. They provide authentication, message integrity, and message confidentiality. SMTP does not define any security features and is known to be vulnerable to forged messages. Privacy Enhanced Mail (PEM) provides similar security services for SMTP to those included in X.400, including protection against forgery, tampering, and unauthorized disclosure, and implementations are beginning to appear. In network management, the OSI CMIP includes provision for authentication, access control, data confidentiality and data integrity. SNMP does not currently provide much security, but authentication and access control mechanisms have been defined for the next version. The OSI Directory Services, X.500, includes authentication services and access control, though has not been implemented significantly in the marketplace at this time. The IPS Domain Name System does not include any security services, though a working group in the IETF is directly addressing this problem presently. Overall, more progress has been made in OSI than in IPS in defining security. The Government has invested significantly in OSI security initiatives. Implementations of the security features in OSI products, although slow initially, are starting to be available. In the Internet, the IETF now considers security to be its most important area of work, and significant work is underway to define standards for security, and to add security to all major network protocols.

With respect to the security situation in the operational Internet, the infrastructure is highly vulnerable to a variety of threats. Most fundamental routing protocols and elements are largely unprotected. Directory services, particularly the Domain Name System, are similarly unprotected. The IETF is just beginning security work in these two areas. Driven by widespread usage and rapid commercialization, it is likely that the next two or three years will see significant improvement in the operational Internet security situation, particularly aimed at a reduction in the vulnerability of the infrastructure. Internet hosts

lack the kind of standard, end-to-end encipherment protocols that they need to protect a variety of applications. However, even if these existed, end systems have many other security problems unrelated to protocol standards. Most security vulnerabilities in Internet hosts stem from problems in specific implementations and in host configuration and management practices. In both of these areas, OSI has no inherent claim to be more secure. Lack of confidence in the security of the Internet and of hosts has led to the growing use of firewalls between the Internet and private organizations or agencies. Firewalls restrict traffic to certain applications, such as e-mail, and may also prevent the use of new applications, such as gopher and World-Wide Web.

Security is a potential limiting factor in Government internetworking and the evolution to the NII, and needs greater emphasis. The critical issues in network security transcend the specific protocol suite in use. They include deployment and policy concerns. The Government needs to accelerate the deployment of available security capabilities and infrastructure for the support of network security services. Increased attention is needed to providing protection of network infrastructure assets and information from unauthorized access. U.S. security policies in such areas as cryptography, key escrowing, export control, digital signature standard and patents need to be addressed and evaluated as an integral part of the security solution development and deployment process.

### 5.3 Technical Sufficiency

Both IPS and OSI are satisfying many Federal Government requirements. Deployment of OSI is less extensive than the use of IPS. Both the IPS and OSI suites have technical limitations, and no protocol stack meets the full range of present or future government requirements. Both IPS and OSI have limitations in some areas: security; accounting information for cost allocation; transaction processing; and real-time applications.

Current weaknesses of IPS include limited address space and inadequate directory services. A strength of IPS is the speed with which new applications become widely available. This is exemplified by the rapid growth in information searching and retrieval capabilities, such as Gopher, Wide Area Information Servers (WAIS), and World Wide Web. Extensive experimentation is taking place with multicasting (using the multicast backbone or MBone) and with real time video and audio.

Strengths of OSI include an expanded address space, full directory services, and new applications such as Electronic Data Interchange (EDI), as well as formal international acceptance. The major weakness of OSI is that the number of deployed systems is small compared to the number of deployed systems using IPS. There are fewer OSI products in the marketplace, and they are not as mature or well integrated as equivalent IPS products. For example, few host implementations of OSI ship with a built-in CMIP management part or have a full stack of applications that tie together X.500 directory, VT, FTAM, and X.400 as a package that all plays together and is optimized for high throughput and performance. There is pressure to re-engineer products such as FTAM and VT, which are perceived as unnecessarily complicated. Efforts are underway to define and implement a minimal OSI (mOSI) stack that, while conformant, only contains the protocol facilities that exactly match the requirements of the supported applications. Some OSI products are harder to install and configure because of their complexity and the lack of tools and utilities. On the other hand, the number of X.400 and X.500 applications in the Federal Government is increasing. Most of these applications use protocols other than a pure OSI suite. Several agencies have committed to deploy an operational X.500 directory infrastructure (DOD, NASA, and USPS). X.500 directory services are used by IPS applications, as well as by OSI.

Despite the availability of the IPS and OSI protocols suites, proprietary systems continue to play a dominant role for satisfying many requirements. The commercial large-scale transaction processing market, such as reservation and banking system transactions, are dominated by IBM's System Network Architecture (SNA). This is also the case for many Federal Government applications, especially where transaction processing trading partner relationships exist between the public and private sectors. Although the OSI Transaction Processing standard has been defined and initial products are beginning to emerge, it is competing with an already dominant market product. Proprietary electronic mail systems are widespread, particularly within local area networks (LANs). Such e-mail systems offer excellent user interfaces and integration with other desktop applications. External interoperability is usually provided by gateways to SMTP or X.400, although often with reduced functionality or reliability.

The reality is that no single protocol stack meets the full range of government requirements, although IPS, OSI, and proprietary products all have a role. Therefore, agencies need a process for obtaining accurate, quantitative information about market share, commercial and government deployment of products or protocols, and product interoperability, in order to assist agencies in selection.

### 5.4 Technology Trends

A number of important technology trends have a potential impact on the internetworking market. Some key areas in the current Internet, equally applicable to OSI, are scaling, wide-area multicast, and security. The continuing scaling of the size of the Internet will require new approaches to routing and addressing, and to resource management. Future routing systems must recognize the needs of a multi-provider environment. Transition to the next generation IP will likely impact end system implementations. The Federal Networking Council's actions with respect to routing and addressing encouraged agencies to follow the guidance on Classless Inter-Domain Routing (CIDR). New approaches to resource management are needed to permit management by type of traffic (such as video versus file transfer), as well as management of overall bandwidth to users and sites. Although multicast is used on the Internet experimentally, solutions to scalable multicast are needed which can be managed in a multi-provider environment. This may have real impact on both videoconferencing and distribution of information.

Asynchronous Transfer Mode (ATM) technology is evolving rapidly. LAN products are available in the 155 Mbps range, and gigabit speeds will soon be available. Wide area network offerings now use existing DS-3 infrastructure and will incrementally deploy onto Synchronous Optical Network (SONET) as carriers build infrastructure. Primary problems in the ATM area are routing and addressing on a global scale, resource management, multicast, and network management including provider/provider interfacing. All-optical networks offer the potential of unprecedented low-cost bandwidth. Challenges will have to be overcome in both device and network research. Networking challenges include possible new transport protocols for gigabit speeds, input/output interfaces and techniques to deliver gigabits to the workstation, application support software to deliver gigabits to the application, and parallel programming techniques to deliver gigabits to the problem.

There are other areas of rapid change. In wireless access, there are networking issues such as handoff, addressing, and compatibility with wired access. Asymmetrical digital subscriber loop will bring video dial tone to home or office at T1 or fractional T1 speeds on legacy twisted pair wire. The diversity of technologies including ATM, wireless, and satellite suggests that an internetworking architecture that accommodates these transparently will continue to be essential.

## 5.5 Technology Resourcing

There are a number of Federal research and development efforts in internetworking. Interagency R&D relating to the Internet includes work on security, routing and addressing. Several agencies are supporting research in ATM and gigabit networking under the High Performance Computing and Communications (HPCC) initiative. Advanced network infrastructure supporting scientific research in other disciplines is a significant part of expenditures. Because the Internet is the testbed for much government funded and academic networking research, and the Internet standards process is linked to the introduction of new capabilities on the Internet, there is a direct influence on standards. On the other hand, there appears to be no comparable research community influence on the OSI standards process.

Since the government has many high performance applications, it can play a critical role as a leading-edge customer for networking technology. This enables agencies to acquire knowledge and experience with a technology in solving real problems, as well as to reduce the risk to product developers by providing an early market. Current examples are the acquisition of ATM services and the deployment of agency-wide X.400 or SMTP/MIME electronic mail with X.500 directory services. The Panel sees this as an increasingly important government role relative to direct support of R&D, as the government relies more on commercial off-the-shelf technology.

## 5.6 Technical Infrastructure

The Internet infrastructure and the addition of non-technical users is leading to the development of additional protocols, tools, and applications. Examples include directory services, vendors building IPS networking functionality into operating systems, and demands for greater network management capabilities. The development of networked information discovery tools such as Gopher, Wide Area Information Servers (WAIS), and World Wide Web (WWW) is another example. The development and evolution of the IPS is closely tied to that of the Internet itself. The Internet provides the infrastructure that is used for testing new capabilities, and also represents a large market providing a critical mass for communications vendors, applications, and information services. The Internet provides a model for many of the needs for a National Information Infrastructure. The Federal Networking Council (FNC) provides for basic directory and network registration services for the Internet.

Another form of infrastructure support is that provided by GSA in the form of master contracts, working groups, and centrally funded interagency infrastructure. As a result of the NPR, there will be a greater authorization for agencies to satisfy their requirements through the purchase of products from other agencies' contracts. The NPR will also lead to non-mandatory master GSA contracts. GSA administratively supported panels and working groups have been established under the Government Information Technology Services (GITS) working group and the Federal IRM Policy Council (FIRMPoC).

The roles and responsibilities for infrastructure development and operations to support all internetworking services from advanced research and development to leading edge to core/commodity services should be clearly defined and formally assigned. These roles and responsibilities should include infrastructure administration (e.g., certificate/registration management; access revocation; key management; directory maintenance); help desk(s); provisions for and coordination among emergency response activities; operations of multifunction gateways, as required; provisions for value added services (e.g., on-line information locators), as appropriate; and solicitation and award of master contracts, as appropriate. The Panel believes that there are areas where centralization is appropriate but

also feels that decentralization in most cases is appropriate, depending on the specific function being provided, and where the expertise in these functions is located.

### 5.7 Summary and Conclusions

No single protocol suite currently meets the full range of Government requirements for data internetworking, much less the full range of media and communications modes. Both the IPS and OSI suites have strengths and weaknesses, as do proprietary protocols. While a single standard would be preferable, the reality is that there are multiple solutions in networking as in other areas of information technology. Protocols for core government-wide services may be selected from IPS, OSI, future standards, or as a last resort proprietary protocols. These should be selected based on technical and marketplace factors, as well as a protocol's status as a standard, as discussed in section 4.4. Each agency or community within the Government will pursue the solution to meeting their mission requirements based on these government-wide standards wherever possible. A process needs to be in place to provide guidance to agencies on all available sources, based on standards, market assessment of products, and Government infrastructure and plans.

The Panel concluded that there is not a single technology or protocol solution to satisfy all Federal internetworking requirements, and that the integration of services is increasing as technologies mature. The Government should take advantage of opportunities for convergence and integration.

Security is a critical technical area and a potential limiting factor in Government internetworking. The critical issues in network security transcend the specific protocol suite in use, and include deployment and policy issues. The Government needs to accelerate the deployment of available security capabilities and infrastructure for the support of security services.

## 6.0 ECONOMIC CONSIDERATIONS

Early in its deliberations, the Panel decided that using IPS or OSI protocols in their entirety was not a viable solution and, therefore, that a direct cost comparison of the two was not appropriate. However, economic trends, both inside Government and in the marketplace, affect the cost of Government internetworking and a trend analysis can be used to determine the vitality of the existing market for these protocols and their potential for growth, and to provide help in guiding agencies towards cost-effective solutions, especially in the core services areas.

### 6.1 Market Leader

To displace the market's leading products, new products must offer greater capabilities that are needed and can be justified in terms of return on investment. Alternatively, the new products must provide comparable capability with a lower life-cycle cost. The cost of introducing new products must also consider the impact of any changes required to the infrastructure. This point is also made in the NIST functional comparison document.

At this time, a comparison of the economics of OSI and IPS network and transport protocols shows that IPS is clearly the market leader. Furthermore, the transition from TCP to OSI transport protocols is unlikely to occur, because it has associated costs with little gain. The market for both IPS and OSI products is growing; however, there are clearly trends emerging that indicate users tend to favor IPS rather than OSI protocols, especially when choosing low-cost, widely available and reliable transport protocols. Since 1989, user expenditures on TCP/IP have been greater than on OSI, and this trend shows no sign of changing. TCP/IP is also fast becoming a direct competitor of well established proprietary transport protocols available from numerous vendors. There is a trend for networking software in the form of TCP/IP to be bundled as an integral part of operating systems to support distributed computing.

Today, a network planner must consider how far into the future protocols will continue to be adaptable to changes in their network. This means selecting transport protocols that are expected to remain popular. Rising demand for the protocol results in a larger supply, which gives the additional benefit of obtaining popular protocols at lower costs. Most users are choosing TCP/IP and not OSI for network transport protocols based on business, not technical, reasons. These business reasons include ready availability from multiple vendors, less risk of obsolescence, and lower cost. Trend surveys show that many large-system users have dropped older proprietary transport protocols in favor of using TCP/IP.

The capabilities of the IPS and OSI suites are sufficiently similar at the network and transport layer that there is little incentive for TP4/CLNP to displace TCP/IP which has a much larger market share. There is more distinction in capabilities between the two suites among the applications, but an issue is how much the additional functionality of OSI applications is needed versus the simplicity and greater installed base of corresponding IPS applications. The OSI applications with additional capabilities that are clearly in demand are the X.400 message handling system and X.500 directory services.

### 6.2 Native Protocols

Internet protocols are now more likely to be used by vendors as native protocols at some layers rather than protocols that have to be dealt with using various gateways. On the other hand, OSI protocols are predominantly solutions that are accessed using gateways. Most LAN operating systems for workstations and personal computers provide TCP/IP as a native transport protocol or allow TCP/IP to co-exist with whatever native protocols they

do use. However, OSI network compatibility is limited to only a few LAN operating systems and even some of those do not offer OSI transport protocols.

The most widely used and available OSI protocol, X.400, is primarily used as a network backbone protocol for exchanging e-mail between different mail systems over a wide area; however, most of the different e-mail systems providing access to the X.400 mail backbone do so with application gateways with associated functionality loss.

### 6.3 Product Development

The Panel believes that U.S. corporations are spending and are planning to spend more network standards and product development dollars on developing and enhancing capabilities for IPS protocols rather than for equivalent OSI protocols. Some U.S. vendors that provide communication protocols have even turned over development of OSI products to third-party vendors in response to low demand for OSI capabilities. Vendors are investing in the development of OSI applications such as X.400, X.500, and EDI which have greater capabilities than, or no equivalent, in IPS, and for which there is customer demand.

Further evidence of this trend is seen in vendor attendance at relevant meetings: vendor attendance at IETF meetings has increased, while at the same time it decreased at American National Standards Institute (ANSI) OSI meetings and at Open Systems Environment (OSE) Implementors Workshops (OIWs). There is now a shortage of OIW vendor volunteers who are active in OSI standards development.

### 6.4 Cost

Today it is difficult to compare directly the costs for obtaining IPS capabilities with the costs for equivalent OSI capabilities, because IPS protocols are usually bundled in with the cost of a workstation or a personal computer's operating system, whereas OSI services are provided as separately priced options. The Government has numerous active contracts where this situation exists. Workstation vendors now provide the UNIX operating system with TCP/IP and network services such as Network File System (NFS), Simple Mail Transport Protocol (SMTP), and File Transfer Protocol (FTP) at no additional charge. Similar OSI capabilities for the same UNIX workstation are separately priced options. Personal computers are also often provided to the Government by systems integrators with IPS services bundled into the price with the MS-DOS or UNIX operating system, while OSI services are available as options.

The Government's requirement for certification of GOSIP products has resulted in the Government paying more for OSI products and in vendors being reluctant to provide OSI services because of the costly and time-consuming certification process. Government acquisitions still allow and often encourage vendors to offer TCP/IP and other protocols besides OSI on the same contract. Often, protocols such as TCP/IP and X.25 (X.25 is considered an OSI protocol) are not required to pass a certification test. The rationale used by the Government to avoid the certification process, except for selected OSI protocols, is that Government is comfortable with the non-OSI protocols, because the non-OSI protocols are already in use in existing Government networks. In contrast, the OSI products have yet to see widespread operational deployments that would detect and correct interoperability issues.

A recent cost study examining life-cycle costs of commercial standards-based and proprietary messaging products showed that X.400 products from several well known vendors were competitive with popular LAN-based proprietary mail systems, as well as with SMTP-based systems. The study showed that initial acquisition costs represent only about 23 percent of the total five-year, life-cycle cost, and that the key drivers of the life-cycle costs were the recurring yearly costs for operations, upgrades, and maintenance. Also, the client software acquisition costs represented only about 4 percent of life-cycle cost.

## 6.5 Summary and Conclusions

Early in its deliberations, the Panel decided that choosing between protocol suites in their entirety was not a viable solution because neither meets the full range of Government needs. Therefore, the Panel did not look at the economic impact of choosing one entire suite or another. Economic issues are one factor of many to be considered in choosing the internetworking solution most appropriate to meeting agency mission requirements. The Panel believes that IPS products on the whole are generally cheaper to acquire than their OSI based counterparts, increasingly so because of the tendency to bundle IPS support in vendor's operating systems, while OSI products remain extra cost items. Minimizing the number of protocols supported, both open and proprietary, is a key issue in life-cycle costs.

For the next several years, the Panel expects users' demands for IPS products to continue to escalate and result in an increased number of new applications that work with IPS protocols. The Panel does not expect demand for OSI products, in general, to surpass that for equivalent IPS products that are well established and meeting most users needs, (e.g. IP, TCP, TELNET, and FTP). However, OSI applications that satisfy unmet needs (either new applications, or needed additional capability) are being implemented by users (e.g. X.400, X.500, EDI).

Since the Panel expects multiple protocol suites to be maintained in Government networks for a long time, a key consideration for network administrators is achieving a minimum number of different protocols while optimizing interoperability and decreasing operating expense. An increase in the number of protocols that must be supported results in increasing the costs associated with networks. Furthermore, the purchase prices for networking protocols and applications are the smaller amount of the life-cycle costs than the costs of operational support, upgrades and maintenance. Finally, maintaining redundant protocol suites produces unnecessary expenses, especially when an expensive and not widely used product is mandated.

## 7.0 RECOMMENDATIONS

Based on the discussion and conclusions in previous sections of the document, a summary and conclusions are provided relative to the issues raised in the charter. This is followed by specific recommendations structured according to the organization with suggested responsibility for the action.

### 7.1 Summary and Conclusions

The Panel's conclusions are restated below relative to the issues raised in the charter.

**Long-Term Issues.** The long-term goal of harmonizing on a single standard for each function, and the interests of vendors and users, would be better served if the JTC1, ITU-T, and IETF would agree to work together in a way that combines the strengths of each organization's process and on a mechanism for recognizing the IETF's technical work. The IETF would benefit from the formal recognition of standards resulting in acceptance by governments worldwide, and ISO and ITU-T would benefit from the technical success of the IETF standards process and its influence on the open systems marketplace. The U.S. Government should use all its influence with the various standards bodies to bring the current discussions between them to a mutually acceptable solution.

**Short-Term Issues.** To address near-term issues of interoperability between the two protocol suites, it is recommended that the IETF and JTC1 SC 6 jointly establish convergence workshops that take advantage of the best characteristics of both organizations. There are two areas where immediate attention is warranted to start to bring together the existing IPS and OSI stacks: an agreed internetworking protocol to replace IP, and a transport layer interface, replacing RFC 1006, so that OSI and IPS applications can co-exist over a common transport protocol.

**Requirements.** The range of Government requirements is not satisfied by any single protocol suite. The IPS and OSI stacks each have capabilities and market share in certain functions that are not matched in the other stack, making a single stack solution unrealistic. The Government should select appropriate applications from both IPS and OSI based on technical and marketplace factors.

**Security.** Network security issues that transcend the specific protocol suite need greater emphasis. Infrastructure and policy issues need to be addressed to accelerate the deployment of security capabilities.

**International Commitments.** Some Federal agencies, such as the FAA, have major international commitments based on the use of OSI protocols. Other agencies, such as NASA and NSF, depend heavily on the IPS and Internet. Protocols from either suite should be available for use, depending on the requirements and infrastructure. Proposed changes to the current GOSIP policy should also be advocated with international partners such as NATO and IPSIT.

**Proprietary Protocols.** Selection of a protocol for government use should be based on technical and marketplace factors, as well as the protocol's status as a standard. In areas where no standards exist, or the standards are not supported by multiple vendors, de facto or proprietary protocols may be the only economic alternative. In such cases, standards with publicly available specifications are preferable so as to allow an open market.

**Economic Impacts.** Due to the difficulty in obtaining adequate data, the Panel is unable to make definitive statements about the economic impacts of alternate scenarios. However, several economic drivers can be identified. Products with significant market share and available from multiple vendors tend to be lower in cost, so selection of protocols for government use should be based on marketplace factors as well as status as a standard. The procurement costs of protocols are dominated by life cycle maintenance costs, which are driven in large part by the number of protocol suites to be supported.

**Testing.** The Government should be primarily concerned with the interoperability and robustness of products. Conformance testing should be primarily a vendor responsibility to warranty their products. A limited range of interoperability testing options would permit users to choose the degree of assurance they need relative to cost. NIST should collaborate with fellow IPSIT members on the international harmonization of the warranty of products.

## 7.2 Specific Recommendations

The vision that the Panel sees for Federal internetworking is that it evolves as a portion of the National Information Infrastructure, providing a full range of integrated communications connectivity (data, voice, video, fax, etc.) among Federal agencies and between Federal agencies and the public and private sector. The Panel believes that three strategic areas are key to attaining this vision. First, there must be increased integration across Federal agency internetworking activities. Second, policies and technology assessments must be refocused toward a more integrated and rapidly evolving telecommunications infrastructure. Third, responsibility for the operational support of the evolving infrastructure must be better defined and formalized. The Panel offers the following specific strategic recommendations in each of these areas, as well as additional tactical recommendations:

**Recommendation 1. The role of oversight and guidance for integration across Federal agency internetworking should be strengthened.**

The objective of this recommendation is better coordination of interoperability across agencies in planning, resourcing, use of standards, technology transition, policy, and oversight. Responsibility for implementing this recommendation lies partly with the Office of Management and Budget (for resources, policy, and oversight), and partly with the Information Infrastructure Task Force (for planning). Some functions could be delegated (such as standards to NIST).

Specific activities in this area include the following:

- Federal Government policy with respect to internetworking; for example, roles and relationships of agencies with respect to FTS-2000, the Internet, and commercial networks in the provision of Government services to the public.
- Guidance for integration; for example, planning for Government-wide services that span multiple backbone networks.
- Budget review and support of incentives for agency initiatives that contribute to improved Federal internetworking. OMB should provide guidance to ensure monetary resources are available to carry out the plans and infrastructure in accordance with a coordinated Government-wide strategy.
- Publication of an annual report by OMB that provides a single, integrated view of agency internetworking and interoperability across the Government and to the public. This would become in effect the strategy and progress report for Government-wide interoperability goals and achievements, and would hold agency accomplishments up to public scrutiny and accountability.

**Recommendation 2. The roles and responsibilities for fostering standards should be refocused and strengthened by the Department of Commerce.**

This should include expansion of activities across all internetworking stages from advanced research and development to leading edge to becoming core/commodity services. Particular emphasis should be placed on expanded and fully coordinated participation in standards forums (including consortia); encouraging convergence towards a single standard, where appropriate; market assessment; and international harmonization of streamlined testing that permits users to choose the degree of confidence they need relative to cost.

**Recommendation 3. The roles and responsibilities for infrastructure development and operations to support all internetworking services from advanced research and development to leading edge to core/commodity services should be clearly defined and formally assigned through the Information Infrastructure Task Force.**

These roles and responsibilities should include infrastructure administration (e.g., certificate/registration management, access revocation, key management, directory maintenance); help desk(s); provisions for and coordination among emergency response activities; operations of multifunction gateways, as required; provisions for value added services (e.g., on-line information locators), as appropriate; and solicitation and award of master contracts, as appropriate. The Panel believes that there are areas where centralization is appropriate, (e.g. registration authority and root name servers) but also feels that decentralization is appropriate in most cases due to the broad range of Federal requirements in the infrastructure areas. The choice of centralized versus decentralized depends on the specific function being provided and where the expertise in these functions is located. The investment in information infrastructure should be coordinated by the IITF.

**Recommendation 4. The roles and responsibilities of affinity groups should be defined, including how they are identified and coordinated, by the Government Information Technology Services Working Group.**

Because affinity groups are the context within which interoperability is important, active participation of affinity groups is required in the selection of standards and in the development of infrastructure to support interoperability. Building on the affinity groups already established in connection with implementing the NPR recommendations, the process for identifying affinity groups, a structure for coordinating them, and their roles and responsibilities needs to be defined. This task falls under the responsibility of the IITF, and specifically the Government Information Technology Services (GITS) Working Group. The several affinity groups working on Government-wide subjects, such as electronic mail and EDI, will need to work closely with NIST in the selection of standards for inclusion in the broadened GOSIP. Affinity groups focusing on specific applications will assume increased responsibility for working with voluntary standards organizations and for selecting the standards they use in addition to the core standards included in the broadened GOSIP.

**Recommendation 5. The current GOSIP policy should be replaced with a new FIPS that includes appropriate standards drawn from both the OSI and IPS protocol suites.**

The selection of protocols for a broadened GOSIP should be based on technical and marketplace factors, as well as on a protocol's status as a standard. Since no single

protocol suite meets the full range of Government requirements, appropriate standards should be drawn from both the OSI and IPS. The scope of GOSIP should be limited to the network and transport layer, and to those applications needed for core government-wide services and for government interoperability with the public. The applicability statement in GOSIP should be modified such that protocols in a broadened GOSIP are mandatory for consideration for use. Convergence workshops should be established to develop technical solutions to the interoperability issues resulting from the acceptance of protocols from both OSI and IPS. The Government's focus should be on interoperability testing with conformance testing primarily a vendor responsibility.

**Recommendation 6. A permanent steering group should be established to review annually the Federal agencies' progress towards achieving the internetworking vision outlined in the Report. The existing FIRP Panel could also be made available to consult and coordinate with agencies working to implement the strategic and tactical recommendations of the report, to help ensure that the full vision of the report is accurately understood and communicated.**

The Panel recognizes that it will be some months before all the recommendations contained in this report can be implemented. Continuing visibility is recommended into the interpretation and implementation of the recommendations since they are interdependent and implementing some but not all of them will not accomplish the objectives. A steering group should be established to provide the continuing assessment of agencies' progress towards achieving the vision. The group's review of agency implementations would be aimed at identifying any gaps or shortfalls in the planned activities or resourcing that would derail this vision from being achieved. The steering group should consist of people who are responsible for achieving the internetworking vision in their own agencies, including at least some of the members of the original Panel, to avoid any future divergence between infrastructure, the marketplace, and standards policy.

## LIST OF REFERENCES


Cargill, C. F., *Information Technology Standardization*, Digital Press, 1989

General Services Administration, *Federal Internetworking Requirements,* January, 1994.

Gore, Albert, Vice President of the United States, *Report of the National Performance Review,* September 7, 1993.

Hogan, M. D., *Information for Standards Process Discussion,* November 12, 1993.

Information Infrastructure Task Force, *The National Information Infrastructure Agenda for Action,* September 15, 1993.

Internet Architecture Board and Internet Engineering Steering Group, *The Internet Standards Process,* Revision 2, RFC 1602, March 1994

Lottor, M., *Communication concerning February 1986 Internet data,* December 1993.

National Institute of Standards and Technology, *Federal Information Processing Standards Publication 146-1, Government Open Systems Interconnection Profile (GOSIP),* Federal Register, April 3, 1991, pp 13626-13627.

National Institute of Standards and Technology Computer Systems Laboratory, *Functional Comparison of the Internet Protocol Suite and the OSI Protocol Suite,* October 15, 1993.

Office of Management and Budget, *Federal Participation in the Development and Use of Voluntary Standards.* OMB Circular A-119, Revised, October 1993, Federal Register, October 26, 1993 pp 57643-57648.

Office of the Vice President, *National Performance Review Accompanying Report, Reengineering Through Information Technology*, Draft, November 1993.

Postel, J., *Internet Official Protocol Standards,* RFC 1540, October 1993.

Reynolds, J., and J. Postel, *Assigned Numbers,* RFC 1340, July 1992.

Rose, M. T., D. E. Cass, *ISO transport services on top of the TCP: Version 3.* RFC 1006, IETF, May 1987.

Widmeyer, S., (Merit), *Communication concerning December 1993 Internet data,* December 1993

# APPENDIX

## Charter for Panel on Federal Internetworking Requirements

### Introduction

The Panel on Federal Internetworking Requirements is appointed by the National Institute of Standards and Technology (NIST). The Panel will study issues and recommend actions which the Federal Government can take to address the short and long term issues of interworking and convergence of networking protocols -- particularly the Internet Protocol Suite (IPS) and the Open System Interconnection (OSI) protocol suite, and where appropriate, proprietary protocols.

The scope of the Panel's work is to identify the Government's internetworking requirements (e.g., security, ease of use, national and international connectivity, sound standards-maintenance procedures), evaluate the current and potential fit between those requirements and the two protocols suites, evaluate alternative scenarios for interoperability and convergence between the two protocol suites, and identify and analyze the cost to agencies of possible Government responses to alternate scenarios. The Panel will produce a report containing its recommendations and will identify policy or regulatory issues which are beyond its purview.

Formation of the Panel was endorsed by the Federal Networking Council (FNC) and the Federal Information Resource Management Policy Council (FIRMPoC) and the Office of Management and Budget asked NIST to charter the Panel. Panel members were selected from nominees provided by the FNC and FIRMPoC to represent the mission interests and requirements of Federal agencies.

### Charter

The Panel will address the short and long-term issues related to internetworking and convergence of the Internet and Open Systems Interconnection protocol suites. At the present time the two are not interoperable. Each protocol suite has its strengths and weaknesses in terms of meeting Federal internetworking requirements. Related issues to be addressed include:

- The comparative strengths and weaknesses of the OSI and Internet Protocol suites and requirements for proprietary products to gateway with them;
- Ease of use of the OSI and Internet protocol suites and required supporting infrastructure;
- The role of proprietary or other protocols not in the OSI and Internet suites;
- Federal security requirements;
- Federal networking requirements at the national and international levels;
- Economic impacts of alternate procurement and deployment scenarios; and

- Relationships and commitments to other entities (such as NATO, IPSIT and IGOSS).

The Panel will seek views of the public and private sectors to obtain the perspectives of Government and industry.

**Recommendations of the Panel**

The Panel will evaluate the current and potential fit between the Government requirements and the two protocol suites, and will make recommendations on the following subjects:

- Feasibility of alternative scenarios for coexistence, interoperability, and convergence between the two protocol suites;

- Expected cost and impact to mission agencies if alternate scenarios are implemented;

- Process to be followed in obtaining advanced Government requirements and in using Federal investments in research, development and infrastructure to best effect Federal requirements;

- Source of specifications for the Federal Information Processing Standards (FIPS);

- Testing requirements for FIPS (conformance and/or interoperability); and

- Procurement and deployment scenarios.

The Panel is also encouraged to identify and describe policy and regulatory issues that it believes need to be addressed but are beyond its purview.

**Panel composition and work schedule.**

The Panel will be chaired by Diane Fountaine, Department of Defense. The Panel members will be:

- Jason Canon, Department of the Treasury

- Michael Corrigan, General Services Administration

- Walter Houser, Department of Veterans Affairs

- William Hughes, Department of Commerce

- Richard desJardins, National Aeronautics and Space Administration

- Milo Medin, National Aeronautics and Space Administration

- Thomas Rowlett, Department of Energy

- Stephen Wolff, National Science Foundation

The Panel will start meeting in October 1993 and is expected to complete its report in early January 1994. The Panel will be assisted by a GSA secretariat.

**Disposition of the Panel's recommendations.**

The report containing the Panel's recommendations will be submitted to Mr. James Burrows, Director of the Computer Systems Laboratory, National Institute of Standards and Technology (NIST). NIST will make the report available to the public, consider the recommendations of the Panel, and then announce any proposed implementation actions in the Federal Register. NIST will solicit public comments before implementation of recommendations or other actions which are within the scope of the authority of the Department of Commerce and/or NIST.

Issues related to Federal policy or regulation will be referred to the Office of Management and Budget for consideration and referral to appropriate authorities for action and resolution.

## GLOSSARY

| | |
|---|---|
| **ANSI** | American National Standards Institute |
| **ARPA** | Advanced Research Projects Agency |
| **ASC** | Accredited Standards Committee |
| **ATM** | Asynchronous Transfer Mode |
| **ATN** | Aeronautical Telecommunications Network |
| **BISDN** | Broadband Integrated Services Digital Network |
| **CCITT** | International Telegraph and Telephone Consultative Committee |
| **CICS** | Customer Information Control System |
| **CIDR** | Classless InterDomain Routing |
| **CLNP** | Connectionless Network Protocol |
| **CLNS** | Connectionless Network Service |
| **CMIP** | Common Management Information Protocol |
| **COTS** | Commercial off-the-shelf |
| **DCE** | Distributed Computing Environment |
| **DNS** | Domain Name System |
| **DoE** | Department of Energy |
| **EDI** | Electronic Data Interchange |
| **ES-IS** | End System to Intermediate System |
| **FAA** | Federal Aviation Administration |
| **FDDI** | Fiber Distributed Data Interface |
| **FIPS** | Federal Information Processing Standard |
| **FIRMPoC** | Federal Information Resources Management Policy Council |
| **FIRP** | Federal Internetworking Requirements Panel |
| **FNC** | Federal Networking Council |
| **FTAM** | File Transfer Access and Management |
| **FTP** | File Transfer Protocol |
| **FTS2000** | Federal Telecommunications System 2000 |
| **GITS** | Government Information Technology Services |
| **GOSIP** | Government Open Systems Interconnection Profile |
| **GSA** | General Services Administration |
| **HPCC** | High Performance Computing and Communications |
| **IAB** | Internet Architecture Board |
| **IDRP** | Inter-Domain Routing Protocol |
| **IEC** | International Electrotechnical Commission |
| **IEEE** | Institute of Electrical and Electronic Engineers |
| **IESG** | Internet Engineering Steering Group |
| **IETF** | Internet Engineering Task Force |
| **IGOSS** | Industry and Government Open Systems Specification |
| **IP** | Internet Protocol |
| **IPS** | Internet Protocol Suite |
| **IPSIT** | International Public Sector Information Technology group |
| **IRM** | Information Resources Management |
| **IRTF** | Internet Research Task Force |
| **ISDN** | Integrated Services Digital Network |
| **IS-IS** | Intermediate System to Intermediate System |
| **ISO** | International Organization for Standardization |
| **ISOC** | Internet Society |
| **IT** | Information Technology |

| | |
|---|---|
| **ITU** | International Telecommunication Union |
| **ITU-T** | International Telecommunication Union - Telecommunications Standardization Sector |
| **JTC1** | Joint Technical Committee 1 |
| **LAN** | Local Area Network |
| **MBONE** | Multicast Backbone |
| **MIME** | Multi-media Internet Mail Extensions |
| **MSP** | Message Security Protocol |
| **NACISA** | NATO Communications and Information Systems Agency |
| **NAFTA** | North American Free Trade Agreement |
| **NASA** | National Aeronautics and Space Administration |
| **NATO** | North Atlantic Treaty Organization |
| **NFS** | Network File System |
| **NIC** | Network Information Center |
| **NII** | National Information Infrastructure |
| **NIST** | National Institute of Standards and Technology |
| **NIUF** | North American ISDN Users' Forum |
| **NLSP** | Network Layer Security Protocol |
| **NOAA** | National Oceanic and Atmospheric Administration |
| **NOSIP** | NATO Open Systems Interconnection Profile |
| **NPR** | National Performance Review |
| **NSF** | National Science Foundation |
| **NTIA** | National Telecommunications and Information Administration |
| **ODA** | Office Document Architecture |
| **OIW** | OSE Implementors Workshop |
| **OMB** | Office of Management and Budget |
| **OSE** | Open Systems Environment |
| **OSF** | Open Software Foundation |
| **OSI** | Open Systems Interconnection |
| **OSPF** | Open Shortest Path First |
| **PEM** | Privacy Enhanced Mail |
| **R&D** | Research and Development |
| **RAM** | Reliability, availability, and maintainability |
| **SDH** | Synchronous Digital Hierarchy |
| **SDNS** | Secure Data Network System |
| **SMTP** | Simple Mail Transfer Protocol |
| **SNA** | Systems Network Architecture |
| **SNMP** | Simple Network Management Protocol |
| **SONET** | Synchronous Optical Network |
| **T1** | Accredited Standards Committee for Telecommunications |
| **T1** | 1.544 Mbps Carrier Standard |
| **TCP** | Transmission Control Protocol |
| **TELNET** | Telecommunications Network |
| **TLSP** | Transport Layer Security Protocol |
| **TP4** | Transport Protocol Class 4 |
| **UNI** | User-Network Interface |
| **USPS** | United States Postal Service |
| **USTR** | Office of U. S. Trade Representative |
| **VA** | Department of Veterans Affairs |
| **VT** | Virtual Terminal |
| **WAIS** | Wide Area Information Servers |
| **WHOIS** | Who is |
| **WWW** | World Wide Web |
| **X3** | Accredited Standards Committee for Information Processing Systems |

| | |
|---|---|
| **X.25** | CCITT Recommendation for Packet Mode Interface |
| **X.400** | OSI Message Handling System |
| **X.500** | OSI Directory |
| **XPG** | X/Open Portability Guide |