WHC-SP-1152

Sitewide Task Team Report for Internet Policy

D. R. Aichele

Date Published
March 1995

Prepared for the U.S. Department of Energy
Office of Environmental Restoration and
Waste Management

Westinghouse Hanford Company
P.O Box 1970
Richland, Washington

Hanford Operations and Engineering Contractor for the
U.S. Department of Energy under Contract DE-AC06-87RL10930

Available to the U.S. Department of Energy
and its contractors from
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831
(615) 576-8401

Printed in the United States of America

DISCLM-3.CHP (1-91)

RELEASE AUTHORIZATION

Document Number:	WHC-SP-1152, Rev. 0
Document Title:	Site-Wide Task Team Report for Internet Policy
Release Date:	03/24/95

This document was reviewed following the procedures described in WHC-CM-3-4 and is:

APPROVED FOR PUBLIC RELEASE

WHC Information Release Administration Specialist:

V. L. Birkland — V.L. Birkland

3/24/95 — Date

EXECUTIVE SUMMARY

The Internet is rapidly becoming the standard for communications, information transfer, and information sharing among U.S. Department of Energy (DOE) organizations. It has long been used by the major laboratories, but is now beginning to be used by headquarters staff to communicate with field offices and contractors and as the access point to DOE's repositories of information. It will soon become key to efficient conduct of operations. Sites without effective access to the Internet will have to rely on secondary, less effective communications means. Therefore, the task team believes it is essential that Hanford become a full participant in utilizing this resource.

This is based on the assumption that the Internet (or its successors) will become the primary means by which Hanford shares information with others and an important means of receiving information from others.

To make this happen, two things are needed. First, an effective access and delivery infrastructure must be provided to DOE and contractor staff. It should be robust, user friendly, yet secure. Second, standard ways of doing business on the Internet to facilitate the interchange of information are required.

Much of the technology exists today for robust electronic interchange of information. The use of this technology needs to be expanded and coordinated throughout the DOE and Hanford contractor community.

Today, staff can make use of electronic mail and bulletin boards and access a broad variety of useful information (e.g., phone directories, excess

equipment lists, and various databases) via the Internet. At the present, these are critical to a small number of programs and projects and have some value to others, but are not yet considered essential. As the use of Internet within DOE is advancing rapidly, it will become the preferred method for communication and information sharing in the near future (within 5 years).

What we see today is a very limited precursor to an entire new way of communicating as well as providing and receiving information that is faster, better, and ultimately cheaper than existing methods.

The conclusion of the Internet Inter-Contractor task team is that the use of the Internet is essential to communicate as well as provide and obtain information and knowledge. The Hanford Site must foster, support, and implement necessary changes to the technology infrastructure to improve user access, maintain security, and assure we are effective participants in the networked community.

Hanford Site contractors should continue to team together to achieve operational and cost effectiveness, appropriate use and security, and investigate and implement the new and effective uses for Internet onsite.

CONTENTS

CONTENTS (continued)

1.0 BACKGROUND/INTRODUCTION

In September 1994, the U.S. Department of Energy (DOE) - Richland Operations Office (RL) Site Infrastructure Division, launched an initiative to develop a Sitewide policy for Internet use and access. Boeing Computer Services, Richland (BCSR) was asked to lead the effort to address Internet use on the Hanford Site.

2.0 STRATEGY

A multi-contractor team was formed with participation from DOE, BCSR, Westinghouse Hanford Company (WHC), Pacific Northwest Laboratory (PNL), Kaiser Engineers, Hanford (KEH), Hanford Environmental Health Foundation (HEHF), Bechtel Hanford Incorporated (BHI), and Mactec. The team's focus was to evaluate several opportunities and issues surrounding use of the Internet, make recommendations for a managed evolution to an Internet work environment, and identify future roles.

The initial meeting of this task team took place on October 4, 1994. At the meeting, a facilitated session was held to identify current Internet use and issues related to Hanford's Internet use. These issues were then grouped into six main categories:

- Benefits/Drivers
- Acceptable Use Policy
- Security
- Cost
- Administration
- Technology

Follow up meetings were held to secure input for development of goals and deliverables for each issue.

For each of the identified categories, contractor sub-teams were formed that reported to a designated main task team lead. The sub-teams would be responsible to accomplish the objectives and deliverables developed for each category.

This report addresses the outcome of the six main categories.

3.0 BENEFITS/DRIVERS

3.1 BACKGROUND

Historically, use of the Internet has been dominated by highly technical Hanford professionals. The recent trend is toward increased use of the

Internet by a broader section of the Hanford workforce. Driving this growing use is a dramatic increase in the capabilities of Internet technology.

3.2 OBJECTIVE

Identify for RL and Hanford contractor management the benefits of broader access to, and use of, the Internet.

3.3 DELIVERABLES

A report and high-level briefing identifying key benefits of and drivers for Hanford's use of the Internet including the *Hanford Federal Facility Agreement and Consent Order* (Tri-Party Agreement), programmatic, and DOE.

Identify typical Internet-based resources that benefit Hanford employees in the performance of their duties.

3.4 GENERAL

This report addresses the business drivers and benefits of Internet in a hierarchial manner: from the Administration and the DOE down to some Hanford projects.

3.5 ADMINISTRATION AND U.S. DEPARTMENT OF ENERGY BUSINESS DRIVERS

Upon review of key policy and strategic planning documents [1] [2] [3] from the Administration and USDOE, there are four common themes for improved utilization of the physical and intellectual resources in government, academia, and industry:

- Education
- Access
- Linkages
- Utilization.

Resource Education

- "Develop a communications strategy that helps industry know which resources are available within the Department." [1]

---

[1] USDOE, "Fueling a Competitive Economy," DOE/S-0108, Washington DC, April 1994.

[2] USDOE, "National Performance Review: Internal Report to the Secretary, Volume 1," September 1993.

[3] Clinton, W.J., and Gore Jr., A., "Technology for America's Economic Growth, A New Direction in Building Economic Strength," February 22, 1993.

- "Improve utilization of DOE's extensive energy, science, and technology information resources to educate students. Install directories of the educational resources on major networks such as Internet..." [2]

- "Ensure a flow of knowledge into society..." [1]

Access to Resources

- "Provide scientific and technical energy information through dissemination mechanisms responsive to customer needs, such as teacher networks, use of electronic networks, public television, and outreach vans and buses." [1]

- "Improve overall access to information on departmental activities." [1]

- "Expand access to computerized energy data by using Internet, making vital energy information instantly available to Internet's 10 million users." [2]

- The DOE and other agencies (in addition to the White House) have implemented a program to provide access to government agencies through the World Wide Web (WWW) server.

- Secretary O'Leary stated in her June 26, 1994 press conference that all the discussed documentation would be made available on the Internet for public access.

Linkages to Other Resources

- "Involve the international community to develop a global research facility network." [1]

- "Forge links with other agencies and academia to leverage research benefits and avoid duplication." [1]

- "Fast communication makes it possible for teams to work closely on a project even if the team members are physically distant from each other." [3]

- "The development of public networks such as the Internet and the National Research and Educational Network will contribute significantly to this diversity, enabling government information to be disseminated inexpensively to a broad range of users." [3]

Utilization of Resources

- "Develop a plan to take advantage of current technology--computer, optical, document management, telecommunications--to improve communications, internally and externally." [1]

- "Expand use of inter- and intra-Departmental electronic mail for better communications, cost savings, reduced waste, and sharing information directly with the public where appropriate." [2]

- "Fully utilize research facilities, as appropriate to reduce unit costs." [1]

Summary

It is clear that the administration and DOE are not only committed to their effective use of the Internet, but see it as a central element in their business strategies.

3.6 HANFORD MISSION OVERVIEW

There are three missions at the Hanford Site that are to be performed consistent with the strategies outlined in the above Administration and DOE business driver section:

- Site Cleanup
- Science and Technology
- Economic Transition

The major goals are to:

- Manage and reduce hazards while enhancing worker safety and health.

- Improve mission effectiveness by shortening the overall cleanup schedule and reducing costs by applying new or previously unknown technologies, enhancing work force effectiveness, increasing administrative efficiency, and improving the decision-making processes.

- Increase the taxpayer return on investment by building partnerships and leveraging the resources at Hanford to mutually benefit cleanup, research, the regional economy, and U.S. industrial competitiveness.

Premise

Increased and more timely knowledge gained through the timely and practical import and export of quality information to and from Hanford is key in addressing these goals.

3.7 HANFORD BUSINESS DRIVERS

The Internet is one route whereby employees will be able to obtain (and communicate) information and knowledge that will allow them and their coworkers to be more prepared to:

- Understand, research, develop, and apply new or previously unknown technologies, processes, or lessons learned.

- Understand unknown, known, or new risks and the methods to minimize or eliminate them.

- Understand and support the benefits to the region and the U.S., in addition to Hanford cleanup.

By the increased and more timely import of information:

Hanford will be more aware of the world's resources that may be beneficially linked to the Hanford mission through contracts and procurement, research and engineering collaborations, and technology transfer. These resources include available technology, equipment, facilities, data, information, and knowledge (craft, scientific, engineering) resources.

By the increased and more timely export of information:

The public, industry, other laboratories, academia, and government will be more aware of Hanford (its mission, history, accomplishments, progress, lessons learned), its resource needs, and its available resources.

3.8 EXAMPLES OF SPECIFIC HANFORD PROJECT OR BUSINESS REQUIREMENTS

- The Federal Laboratory Consortium for Technology Transfer (FLC) is Congressionally-chartered to promote transfer of technology from federal laboratories to the private sector. The FLC utilizes the Internet to electronically link over 700 federal laboratories, including PNL and WHC. Electronic mail and a bulletin board (or "roundtable") are presently available throughout the FLC though numerous laboratories are independently establishing additional services such as the WWW. This is driven, in part, by industry aggressively pursuing electronic commerce via the WWW (e.g., TRW, AT&T, IBM, Microsoft, Intel, Electronic Data Systems, Hewlett Packard, Compaq Computer, Apple Computer, SAS Institute).

- In support of the Environmental Molecular Sciences Laboratory (EMSL), the Theory, Modeling, and Simulation Program (TM&S) uses the National Energy Research Supercomputer Center (NERSC) facilities as well as resources at Oak Ridge, and Los Alamos. Similarly, TM&S has many external collaborators who interact frequently with TM&S scientists using Internet to access PNL computers, share data analyses, and perform all phases of research.

- In support of EMSL, the High Performance Computational Chemistry project is one of DOE's High Performance and Communications Initiative, Grand Challenge Applications projects. It is a joint effort between PNL, Argonne National Laboratory (ANL), and five industrial collaborators. On an almost daily basis, the scientist teams discuss software designs, plan and organize workshops, share data, or move software over the Internet. [The principal investigator asserts that the project would likely not have been

funded if Internet resources to connect these seven institutions had not been available]

- During the development of a Cooperative Research and Development Agreement (CRADA) that transfers Hanford equipment to the private sector at a cost savings to the DOE, the private sector participant identified a key piece of equipment, critical to their development efforts, that WHC could not fulfill. An electronic message was communicated from WHC to an information network linked to the FLC. Within 2 days a response was made by Los Alamos National Laboratory (LANL) that matched some of their surplus equipment with the need of the private sector participant. A similar positive response was received from Lawrence Livermore National Laboratory (LLNL) within the week.

- A DOE order is being developed requiring Lessons Learned information to be placed on Gopher (an Internet browser service) servers. The Environmental Safety and Health Technical Information Service (TIS) at Hanford contains Lessons Learned, OSHA orders, Emergency Preparedness, and Site Industrial and Office Safety information that can be accessed through a Gopher server.

- "DOE Methods for Evaluating Environmental and Waste Management Samples," a 700 page report, which has in the past been distributed by paper, has now been made available via a gopher/WWW server, saving printing and distribution costs.

- In support of the Applied Physics Center, the use of Internet was essential in bringing together a broad client base enabling support for $4M in fiscal year (FY) 1994 alone for the Intelligence community.

- As reports of a flaw in the Intel Pentium chip surfaced nationwide, access to the Internet via the proxy server and the cc:MAIL gateway were used to obtain Pentium technical information and test programs from Intel and IBM (as well as numerous other sources). Information that previously would have taken days to obtain via traditional mail, or incur an additional cost to acquire via a paid service such as Compuserve, were acquired in minutes for no additional cost.

- Numerous examples are available of individuals who have found software bug notices, code fixes and work-arounds, new add-on utilities, worldwide telecommunication standards, etc. by monitoring Usenet news discussion groups. Furthermore, resolutions to software problems via the Internet community, were oftentimes faster than the software company "hot lines."

- Computer Support information is now available to Personal Computer (PC), Macintosh, and UNIX users via the gopher/WWW server (PNL Info Server). This reduces the support load, as well as improving response time. For example, we were able to quickly make available a number of references related to the Pentium chip problem.

- There is an increasing number of formal requests by the public and industry for access to DOE and Hanford Contractor information, including declassified documents, through the Internet (e.g., Indian Tribes, several Hanford subcontractors, Associated Western University Northwest). DOE-HQ is addressing these requests, in part, through the OPENNET initiative.

3.9 CONCLUSIONS

Similar to the telephone and Local Area Network (LAN), the INTERNET is becoming integrated as a business tool at Hanford, other federal sites, and the commercial sector. Awareness of its functionality is increasing with nationwide use and development efforts. The question is not if Hanford will use the INTERNET but in what scope and manner to support the DOE and Hanford missions.

THE EXISTING AND EVOLVING INTERNET INFRASTRUCTURE IS AN ESSENTIAL TOOL THAT SHOULD NOT BE IGNORED, BUT TAKEN ADVANTAGE OF.

4.0 ACCEPTABLE USE POLICY

4.1 BACKGROUND

An Acceptable Use Policy (AUP) documents what activities constitute an acceptable use of the given resource, in this case the Internet. For instance, AUPs exist for NorthWestNet, Energy Sciences network (ESnet), and National Science Foundation network (NSFnet), three major constituent parts of the Internet used by Hanford. The primary driver for such an AUP is to define appropriate use of employee time and government computer and network resources.

4.2 OBJECTIVES

Develop and recommend an Internet use policy for Hanford that defines appropriate use of government and network resources and protects user privacy to the largest extent possible.

4.3 DELIVERABLES

An Internet AUP for Hanford that is consistent with applicable DOE policies and orders, contractor policies, and with the use policy of Internet service providers.

Identify training and communication options that contractors can use to promote compliance with the recommended AUP.

4.4 GENERAL/PURPOSE AND SCOPE

The purpose of this document is to convey an AUP regarding utilization of the Internet by Hanford employees. This policy is subordinate to all applicable U.S. Government laws, DOE orders, and AUPs of Hanford's Internet access providers.

4.5 GENERAL GUIDELINES

The Internet is a worldwide collection of networks that connect individual users to Government, commercial, not-for-profit,, and education networks and resources. It contains an estimated 45,000 private and public networks and some 15 to 20 million users. Hanford's internal networks are currently connected to the Internet via DOE's ESnet as the primary provider and NorthWestNet as the secondary provider. In general, the network path being used for a particular access is not known to the user.

ESnet is a national computer data communications network managed and funded by DOE, Office of Energy Research (ER) for the explicit purpose of supporting its scientific research programs. Use of ESnet for bona-fide business activities, which support the DOE/ER mission is acceptable. Use of ESnet is also permitted for work sponsored by DOE Programs that have established a Memorandum of Understanding (MOU) with ER and as otherwise provided for in this policy. An MOU is in place between ER and Environmental Management (EM).

NorthWestNet is a regional computer data communication network serving a consortium of universities, colleges, libraries, hospitals, government agencies, primary and secondary schools, and commercial enterprises in the northwestern United States. NorthWestNet is wholly owned, managed, and operated by the Northwest Academic Computing Consortium (NWACC). PNL's membership in NWACC allows it to "aggregate" Internet access for DOE-RL and other Hanford contractors.

This AUP is intended to ensure Hanford, ESnet, NorthWestNet, and other Internet resources are employed for authorized and funded uses and/or applications.

Acceptable Use of Internet includes:

- Communication among DOE funded principal investigators and their collaborators, regardless of location.
- Access to external scientific facilities for the purpose of conducting DOE funded and/or approved research and education activities.
- Traffic that either originates or terminates within the Hanford Site and complies with the other rules and regulations of this AUP.

- Approved information exchanges and sharing of facilities to permit the use of :
  - Hanford information resources and/or those of another organization.
  - Hanford computational facilities or those of another organization.
  - Video Conferencing between Hanford staff and external collaborators or facilities.
  - Communications between DOE contractors and their subcontractors for the purpose of conducting business in direct support of Hanford programs.
  - Communications between DOE contractors and their parent company for the purpose of conducting business in direct support of Hanford programs.
  - Communications sharing General scientific and administrative information regarding any DOE/ER programs and/or other DOE programs.
  - Communications concerning professional associations, government/university committees, and/or individuals associated with the facilitation and/or conduct of DOE research and education.
- Commercial announcement of products or services of use to the DOE community, where the recipient has specifically requested to be informed of such.
- Any usage conducted under a reciprocal agreement between DOE and other network providers.
- Incidental communications among DOE researchers and their collaborators that contribute to their work.

Unacceptable Use of Internet includes:

- Commercial or for-profit usage not in direct support of DOE activities.
- Personal use not related to the conduct of work on behalf of the DOE.
- Unsolicited advertising of for-profit products and services.
- Lobbying Congress or the Administrative branch for purposes of supporting or not supporting various issues, legislation, programs, or projects.

4.6 TRAINING AND COMMUNICATION

The following are training and communication options identified by the sub-task team.

- Communication and training regarding Internet acceptable use should be the responsibility of the Computer Protection Program Manager (CPPM) in each Hanford organization.
- Each contractor CPPM review existing network access policies and documentation and consider modifying existing policies and/or documentation (e.g., Unclassified Computer Security Manual at PNL) to include the provisions of the AUP.
- Training should become an integrated part of the ongoing unclassified computer security training within each Hanford organization. CPPMs should give consideration to early training as Internet access becomes available.

5.0 SECURITY

5.1 BACKGROUND

The primary concern is protecting Hanford information technology resources from unauthorized access while still maintaining an appropriate ease of use. An additional concern is possible increased frequency of PC viruses from software imported by users from the Internet.

5.2 OBJECTIVES

Ensure that government and contractor information systems are adequately protected from unauthorized access through the Internet. Ensure that authorized use of the Internet is not unnecessarily hindered.

5.3 DELIVERABLES

Evaluate existing Hanford Internet security posture, identifying strengths and weaknesses of current policies, procedures, and technology. If appropriate, recommend an action plan to correct any identified deficiencies or to investigate and pursue technical improvements.

A recommended policy for supporting access to the Hanford Site information resources by authorized external individuals and organizations. The recommendation should include a process for periodically updating that policy in response to technological changes.

5.4 GENERAL

The inter-contractor task team identified security as one of six main issues that needed to be addressed. Personnel at Hanford will be using the Internet and similar tools to conduct their business with an ever expanding community. The primary focus of the security task team is to balance the protection of Hanford information technology resources from unauthorized access with ease of use.

Connectivity with external entities entails a higher level of risk than operating in an isolated environment. Service providers, administrators of information technology resources, and data owners must weigh the benefits of increased connectivity with the potential risks to their areas of responsibility. As an example, there has been an increase in the number of viruses found on Hanford Site computers because offsite connectivity has been available. To date the impact of these virus incidents has been within acceptable limits. Otherwise those responsible for maintaining information resources would have directed service providers to sever connectivity.

The Hanford Site has implemented a "fire wall" concept to protect its information resources from unauthorized access. This approach has adequately protected government and contractor information systems. Improvements are being made to improve Hanford's ease of access to Internet while maintaining a reasonable level of protection from unauthorized users. PNL and WHC have policies and procedures in place that set standards for outgoing and incoming Internet communications. Other contractors must be required, by RL, to use either a PNL or WHC firewall or install their own with the same level of protection provided by one of the existing firewalls. Installation of firewalls with a separate link to the Internet, must be reviewed by other site firewall owners before installation. This review is necessary to avoid network routing problems caused by multiple Internet connections onsite.

The requirements to connect to more locations and take advantage of technology improvements will increasingly require the distribution of telecommunications paths and connections to the work group and away from a single, or few, central connections. These changes will be made to shift accountability to the resource administrator/manager, improve the ability to share information among work groups, permit the work group administrator to tailor resource connectivity to meet unique needs, and to increase ease of use. These changes, while ostensibly improving productivity and ease of use, cause some negative impacts. Consistency of control is more difficult to maintain (and thus more costly), trust relationships between platforms and users of these platforms become more complex, maintenance becomes more difficult and costly with each variation in configuration of these platforms, and the ability to respond to an incident effecting the site becomes more difficult.

Based on the hostility of Internet, security is not good enough. Version 6 of TCP/IP, planned for release in 2005, will address some of today's known weaknesses. However, it may be long after 2005 before Version 6 is available across all platforms. In the interim we need to continue awareness training for users as well as for administrators of computers. We need to take advantage of lessons learned by other computer sites by using services provided by organizations such as CIAC. The level of trust is only as high as

the protection provided by the weakest link. These issues can each be dealt with effectively by the definition and enforcement of site standards for Internet connections and security implementations.

Policy Recommendations:

A standard for contractor firewall implementations must be developed and followed by each contractor. Each implementation should be coordinated with other site firewall administrators to assure that technical problems are not introduced (multiple routing conflicts) and that baseline security requirements are met.

Continue to require that suspected security incidents, including firewalls, are reported.

Continue to enforce the requirements for sensitive/essential computers to have risk assessments, contingency plans and certification by CPPMs.

Develop a consistent policy for the Site on use of software retrieved from the Internet.

6.0 COST

6.1 BACKGROUND

Hanford startup costs for Internet use are variable (based on past investments) and there will be future costs for value added services.

6.2 OBJECTIVES

Ensure that the present cost of Internet access is commensurate with sites requirements and the services being provided. Ensure that Internet access costs are equitably distributed between user organizations (RL and Hanford contractors).

6.3 DELIVERABLES

A list of cost elements and rough order of magnitude (rom) costs for current Internet activities and estimate growth over the next 5 years.

6.4 APPROACH

The emphasis by the team was to identify current and near term expense and capital costs. Costs were reviewed in terms of user contractors and category of technology, which resulted in these lists:

USER CONTRACTORS	TECHNOLOGY
BCSR	CONNECTIONS
DOE-RL	NETWORK INFRASTRUCTURE
HEHF	DE-MILITARIZED ZONE (DMZ) SERVERS
ICF KEH	WORKSTATION/CLIENT SOFTWARE
MACTEC	SUPPORT (END USER)
PNL	
USACE	
WHC	

Preliminary cost data was gathered, then reviewed against current and future technical/operational directions. Costs were broken down into expense and capital dollars and categorized as either nonrecurring or recurring.

6.5 ASSUMPTIONS/EXCLUSIONS

Costs associated with connection to the ESnet, the Site's primary "highway" to Internet, is funded and paid for by DOE-HQ. The anticipated expansion of the T1 line to a T3 line to LLNL in the next 12-18 months will be a DOE-HQ paid project. This funding policy will remain during the 5 year planning period (1995-1999).

No costs are included for PC/Workstation upgrades or additions because primary demand would not be due to Internet requirements.

No costs are included for addressing equipment obsolescence, which may or may not occur during the planning period. It is a factor that needs to be addressed sometime in the future, as does the obsolescence factor of equipment not associated with Internet.

Costs associated with the effective access and utilization of the Internet are management issues and not included as part of this study.

Labor dollars for out-years include a 2.9% escalation factor.

6.6 FINDINGS

Contrary to the initial background statement, the costs associated with Internet are fixed or semi-fixed and not variable. Access cost to Internet are not usage (time) based. The number of users does not significantly affect the infrastructure costs. No true Internet variable costs were identified.

The following conclusion was obtained from the preliminary cost review:

> Technology and applications devised initially for Internet are now becoming a necessity in meeting the internal communication needs within the Site's infrastructure. It is internal demand that will dictate expansion of email gateway usage, increased WWW server application and a move to commercially purchased client software to replace and

augment current public domain software, like MOSAIC. Internet will then piggyback off these changes/upgrades, which are not considered to be Internet demand cost drivers.

With these findings the Internet cost picture over the planning period appears as follows:

Expense Costs (Recurring) in Thousands

TECHNOLOGY						
CONNECTION	1995	1996	1997	1998	1999	Comments
Northwest Net						
Access	37.5	37.5	37.5	37.5	37.5	Half PNL - Half BCSR Supported
T1 Line	37.5	37.5	37.5	37.5	37.5	
Support	15.0	15.0	15.0	15.0	15.0	Paid by PNL
ES Net						
Access	-	-	-	-	-	Paid by DOE-HQ
T1 Line	-	-	-	-	-	Supported by DOE-HQ
T3 Upgrade	-	-	-	-	-	To be Paid by DOE-HQ
Support	8.0	8.0	8.0	8.0	8.0	Paid by PNL
Total	98.0	98.0	98.0	98.0	98.0	
NETWORK/INFRASTRUCTURE	1995	1996	1997	1998	1999	Comments
Maint/Admin.	66.6	68.5	70.5	72.6	74.7	0.5 FTE by BCSR
Total	66.6	68.5	70.5	72.6	74.7	
DMZ SERVERS	-	-	-	-	-	See Nonrecurring Costs
WORKSTATION/CLIENT SOFTWARE	-	-	-	-	-	See Findings
SUPPORT(END USER)	1995	1996	1997	1998	1999	Comments
Training	3.6	3.7	3.8	3.9	4.0	Weekly PNL class (Labor)
Help Desk	20.8	42.8	22.0	9.1	9.3	BCSR start up then level off.
Total	24.4	46.5	25.8	13.0	13.3	
Total Expenses	189.0	213.0	194.3	183.6	186.0	

Capital Costs (Recurring) in Thousands

Technology						
Connection	1995	1996	1997	1998	1999	Comments
Upgrade Pipeline	50.0	50.0	50.0	50.0	50.0	BCSR allowance for changes/upgrades to site network areas

Nonrecurring Costs

Expense - BCSR project ($177K) for FY 1995 to prepare WHC/KEH/BCSR for Internet expansion in areas of Network Infrastructure/DMZ servers/ and Workstation/Client Software.

Capital - BCSR projected ($80K) allowance to expand DMZ server networks in FY 1996.

7.0 ADMINISTRATION

7.1 BACKGROUND

Internet information serving technologies such as the WWW and Gopher represent a new form of electronic information publication. The question before the team was whether current Hanford policies and procedures for information clearance and release are appropriate and sufficient for use with these new technologies.

7.2 OBJECTIVES

Ensure that adequate policies are in place for administering Hanford's Internet services.

7.3 DELIVERABLES

Recommend changes, if needed, to the current DOE and contractor policies and procedures for information release applicable to Internet publishing to ensure effective and efficient use of Internet publishing servers such as WWW and Gopher.

Recommend guidelines for administration of new Internet services that become available.

7.4 FINDINGS AND RECOMMENDATIONS

Existing Policies and Procedures for Information Release

The team reviewed existing DOE orders and contractor implementing procedures covering the release of information outside the Hanford Site. The following were found to be applicable:

DOE Order 1340.1A, *Management of Communications Publications, and Scientific and Technical and Engineering Publications*

DOE Order 1340.1B, *Management of Public Communications Publications*

DOE Order 1430.1D, *Scientific and Technical Information Management*

DOE G 1430.1D-1, *Guide to the Management of Scientific and Technical Information, June 1994*

WHC-CM-3-4, *Information Release Administration*

Author's Guide to Publishing at Battelle.

The above documents outline requirements and provide guidance to Hanford staff who intend to publish information related to DOE funded work performed at Hanford. The bulk of the applicable requirements cover clearance reviews. These reviews are required before information is released to the public. The required categories for review include:

- Security classification and other limited distribution categories
- Proprietary and intellectual property
- Management and technical.

The team believes that the intent of the referenced documents is to address information that is released to the public, regardless of its format or the media it is carried on (e.g., paper, electronic). The language in these documents implies that this is the case.

Recommended Action

The team found that the existing policy and procedures are intended to cover the release of information in electronic form as well as in paper form. We further found that the existing implementing procedures could be easily adapted to clearly apply to the Internet. Therefore, we found no compelling reason to create new policy level documents.

The team recommends that the existing implementing documents be revised to more clearly indicate that they apply to electronic as well as paper media. These documents were identified as WHC-CM-3-4, *Information Release Administration* and *Author's Guide to Publishing at Battelle*. The team did not review similar documents from BHI or HEHF. If they exist, the team recommends that they be similarly revised, if required.

Concurrent with the schedule for this Hanford Internet Task Team, WHC and PNL began revising their procedures. These revisions will be completed during FY 1995. In addition, PNL developed *Guidelines for Placing Information on the Internet* (Attachment A) to specifically address publishing on the Internet and to provide staff with a single document that contains clearance requirements as well as other Internet resource information and contact points. This document is available to staff via PNL's Gopher/WWW server, "PNL Info Server." When DOE and the other Hanford contractors provide general access to the Internet, they also may want to publish some similar guidance on-line.

Guidelines for Administration of New Services

The team recognized the need to have some mechanism for inter-contractor review and implementation of new Internet services. While it's clear that some Internet services are and will be of value to only one contractor, others will be applicable Sitewide. The team did not want to recommend creation of yet another committee to accomplish this, if at all possible.

PNL and WHC have already been sharing this kind of information in an informal fashion as part of ongoing information exchanges between their respective Information Systems groups.

PNL also created documentation on administration of WWW/gopher servers. A standard configuration was selected, tested, and checked for security. A Configuration Guide is available along with a corresponding security plan on the PNL Info Server. In addition, PNL is in the process of drafting a document describing roles and responsibilities for the authors of Internet documents and those involved in the administration of Internet services. This document will also be available on the Internet server.

Recommended Action

The team recommends that the existing informal exchanges be continued and encouraged. We understand that there is some discussion of reinstating the Official Point of Contact (OPC) group. If that comes to pass, the OPC group could provide official concurrence to recommendations made by these information sharing groups.

Aging and Maintenance of Documents

Recognizing that information published on the Internet represents DOE and its contractors to the world and needs to be up to date, the team identified the need for periodic updating or deletion of documents. The team believes that this responsibility rests jointly with the author and the system (or file server or home page) administrator. We also recognize that the intended duration will vary depending on the type of information and type of listing (e.g., bulletin boards, technical articles, high-level capabilities or site descriptions).

Recommended Action

The team recommends that each Internet server administrator establish a time period after which documents will either be automatically deleted or updated by the author, as appropriate.

8.0 TECHNOLOGY

8.1 BACKGROUND

Effective use of the Internet involves a diverse set of established and emerging computer technologies. Opportunities exist to coordinate the introduction and ongoing use of these technologies at the Hanford Site.

8.2 OBJECTIVES

Ensure that responsible Hanford parties maintain cognizance and understanding of current and emerging Internet technologies, and introduce required or strategic Internet technologies to Hanford in a timely fashion.

8.3 DELIVERABLES

A high-level briefing, covering both Hanford and the industry, identifying the current state of Internet technology and a forecast for its future directions.

Develop a strategy for coordination and cooperation among Hanford contractors in the deployment and support of Internet-related technologies.

8.4 GENERAL

Individual computers are joined together into a network, which has limitations on its size and complexity. Individual networks are connected together by internetworking and form an internet. The huge amalgamation of internetworks is called the capital-I Internet.

"Internet technology" is nearly as vast as the Internet itself and consists of at least the following dimensions:

The Internet Hardware & Interconnection - The internet hardware and its configuration is what joins the vast number of individual networks into the Internet. Every Internet site must connect itself to the Internet in some fashion to participate in the greater community. Technology and conventions have evolved to ease the process of sites joining the Internet.

Low-Level Protocols - Protocols are the electronic languages used between computers to allow them to communicate efficiently. At their lowest level most users are totally unaware of protocols, which nevertheless remain all important in computer communications. Although the Internet is multi-protocol it is dominated by the TCP/IP protocol.

High-Level Services - Building on the low-level protocols, high-level services have been defined (or more correctly have grown) on the Internet. These services are what Internet users directly experience and value. Popular services include electronic mail, Usenet newsgroups, FTP, Telnet, Gopher, WAIS, and WWW. An emerging service is video conferencing.

Internet Resources - Building on the basis of hardware and connectivity, protocols, and services a vast array of resources have been made available on the Internet. One cannot easily fathom the depth and breadth of existing Internet resources, which include access to literally millions of people and nearly the full extent of human activity and knowledge.

Attachment B summarizes the technology and issues surrounding Internet connection. The technology team plans on addressing the technological implications of the protocols and services in later versions of this report. Suffice it to say that both WHC-BCSR and PNL plan to support all major Internet services with the implementation at differing levels of maturity.

9.0 ACKNOWLEDGEMENTS

The following were contributing members and task leads.

Benefits and Drivers Team Members:

Dave Greenslade, Acting Lead - WHC
Debbie Aichele - BCSR,
Beth Hetzler - PNL,
Cindy Moody-Brock - BCSR
John Murphy - DOE,
Alan Turner - BCSR
Dan Walker - BCSR,

Acceptable Use Policy Team Members

Bob Mahan, Lead - PNL
Gail Clark - DOE
Lois Holmes - PNL
Jerry Johnson, Resource - PNL
Cindy Moody-Brock - BCSR
Bill Riedeman - MACTC

Security Team Members

Jim Stowe, Lead - WHC
Rick Grandy - BCSR
Dave Kaas - BCSR
Tom Mathieu - PNL
Bruce Oliver - WHC
Collen Tollbom - PNL

Cost Team Members

Dennis Fitzgerald, Lead - BCSR
Russ Barner - PNL
Rick Blancq - USACE
Donna Gibson - BCSR
Rick Grandy - BCSR
Jerry Johnson - PNL

Administration Team Members

Erik Anderson, Lead - PNL
Beth Hetzler - PNL
Jeff Highland - BCSR
Ginny Scorup - WHC
Mike Talbot - DOE

Technology Team Members

Greg Chartrand, Lead - PNL
Rick Grandy - BCSR
Jerry Johnson, Resource - PNL
Dave Kaas - BCSR
Bill Sporcich - BCSR/DOE
Allen Turner - PNL

Technical Consultant

Curt Johnson - BCSR
Tony Sako - BCSR
Alysia Schwarz - BCSR
Bryan Young - BCSR

ATTACHMENT A

PACIFIC NORTHWEST LABORATORY
GUIDELINES FOR PLACING INFORMATION ON THE INTERNET

Welcome to the Universe of Electronic Information

PNL participates in the Internet, a worldwide system of computer networks, systems, and users. You and all other staff members on the PNL network have access to the Internet, which reaches millions of people all over the world.

The Internet contains a galaxy of electronic information. Within this information galaxy are smaller spaces, like Planet PNL -- with two separate hemispheres of information space: public and private. The public sector is available to all Internet users; PNL private information is available only to those on the PNL network. Using viewer tools, everyone on the PNL network can view the contents of the PNL private information space, the PNL public information space, and most of the Internet information.

PNL's public and private information spaces are organized to provide a consistent look and feel. Beginning at the top level in this organization, you can view information and select from a variety of successively more refined topics to find a particular piece of information.

The top level contains documents about PNL as a whole, a structure to help locate information, and entry points into lower level information spaces, such as organization or project information spaces.

Each organization or project information space is a collection of documents within a structure. Each space is managed by a trustee who is responsible for the content and structure of the spaces; the trustee is the point of contact for all issues about the space.

How Can I View Internet Information?

To view information, you need a tool that speaks the correct network language. The PNLInfo Browser tool is provided to PNL as part of IS&S' Electronic Publishing Services. This tool allows users of networked workstations (Windows, Macintoshes, and most UNIX) to view the PNL private information, PNL public information, and external information on the Internet. PNLInfo Browser also allows you to make local copies, print, mark interesting areas for future reference, and subscribe to notification of new versions. More information on this tool is available from *PNL IS&S Customer Service via cc:Mail or by calling 375-6789.

Another viewing tool, NCSA Mosaic, can also be used at PNL by organizations that can internally support the product. This tool is not supported by IS&S at this time, but is compatible with their Electronic Publishing Services strategy. IS&S plans to rollout support for Mosaic or a similar tool in FY 1995.

The Communications directorate maintains a set of PNL "home pages" in Mosiac on the portion of the Internet known as the WWW. These pages can be accessed by millions of Internet users. They contain general information about the Laboratory, publications and press releases, major business areas, and other topics of interest. PNL research staff can have information about their organizations and programs placed on these home pages, or they can develop their own home pages that are linked electronically to the Lab-level home pages. Contact **Pam Novak (376-1243)** or via cc:Mail for more information.

What's the Internet Good For?

The Internet can be an ideal way to gain general knowledge or get answers to specific questions. Here are the types of information PNL is putting on the Internet through the PNL public space, available worldwide:

- overviews of organizations and programs
- press releases
- cleared technical information of broad interest
- pointers to other servers.

Here are the types of information PNL is putting on the internal PNL private space:

- computer support information
- internal newsletters
- descriptions of internal resources and how to access them.

When Should I Think Twice?

The material you place on the Internet becomes a form of advertising for you and for PNL. Many people, including potential employees and potential clients, will be seeing it. Before you put material on the Internet, be sure it is readable, current, accurate, and appropriate for unrestricted public release. Remember that the information we put in the public space is accessible worldwide, including in sensitive foreign countries.

Here are four types of information that probably are <u>not</u> suitable for Internet:

- Information that becomes out-of-date very quickly and requires frequent updates.
- Anything that's classified, business sensitive, strictly private, or simply frivolous.
- Information that is not cleared.
- Information that doesn't belong to DOE or PNL (work done for 1831 clients or in partnership with industry must be approved by the client before it's disseminated via the Internet).

Just as in paper publishing, you must provide proper reference to other work that you cite or use. This need for permission applies to copyrighted text and graphics. Also, avoid obligating persons without their knowledge; for example, publishing their name as a contact or subject matter expert.

Each person who places material on Internet has an obligation not to add unnecessarily to the information mass that slows down users and their computers. Ask yourself what information you find useful when you're browsing on Internet. What wastes your time? What do you wish you hadn't even read? The answers are often good benchmarks to use in deciding what -- and how much -- to put on the Internet.

How Do I Publish a Document?

Publicly published documents must be cleared and assigned a clearance number. The author is responsible for the accuracy and appropriateness of a document. After obtaining clearance, the author contacts the trustee for the appropriate information space. The trustee can further coordinate the publishing process from that point. Typically, the author and trustee need to agree on the following:

- Where in the information space the document will appear
- Format and style of the document
- Contact information and responsibility.

For public information spaces, the trustee must verify that each document contains the required clearance number.

For questions on information space, trustees, and other electronic infrastructure issues, contact **Beth Hetzler (375-6690).**

What Review and Clearance is Required?

PNL's Clearance Office coordinates reviews required by statute, by DOE Orders, or to protect legal interests of PNL and its clients. These reviews are required before information is released outside of the Laboratory, whether in paper or electronic form. The required categories for review include:

- Security classification and other limited distribution
- Proprietary and intellectual property
- Management
- Technical (if required by client).

Certain organizations within PNL often require additional reviews (editorial, technical peer, DOE). The Clearance Office can help you determine the necessary reviews for your material.

The Management Guide (Section 10.1) and the *Author's Guide to Publishing at Battelle* (available through Document Control, 375-2340) contain detailed information on the clearance process.

To expedite the review and clearance of items targeted for the Internet, choose one of these paths: the traditional paper routing or a partially electronic path.

Traditional Paper Routing

- Complete a clearance form and secure signatures from management and the authorized derivative classifier.
- Submit the clearance form and two copies of your document to the Clearance Office (K1-06).
- The Clearance Office will notify you when clearance is completed.

Partial Electronic Path

- Complete a clearance form from the WordPerfect macro (PUBCLEAR.WPM). Include, in the Comment section, instructions on how to access the electronic document (url address, PNL network directory address, file name).
- Print a copy of the completed clearance form and secure signatures from management and the authorized derivative classifier. Forward the printed copy with signatures to the Clearance Office.
- Electronically send the WordPerfect clearance form via cc:Mail to **Darlene Varley**. If your document is in html format, make a note in the comments section of the form giving the URL of the internal PNL server so the reviewers can access it. If your document is in a text format, attach it to the cc:Mail message. The Clearance Office will begin the reviews immediately and will match up the printed copy of the clearance form when it arrives. (NOTE: Do NOT place the electronic document on a fileserver until AFTER it is reviewed by an Authorized Derivative Classifier and determined to be unclassified.)
- The Clearance Office will notify you when clearance is completed.

For questions on clearance, contact **Darlene Varley (375-2853)**.

What is Intellectual Property?

The disclosure of new ideas, techniques, processes, or software (collectively called intellectual property) without first securing adequate protection, can result in its loss. PNL sells and licenses its intellectual property, so we need to be sure that rights are not lost by premature disclosure. Electronic disclosure can be every bit as damaging as printed disclosure. Any information potentially protected as intellectual property should proceed through the clearance process before disclosure. The three most common types of such property are:

1. INVENTIONS subject to patent. If inventions are publicly disclosed before patent applications are filed, patent rights will be lost in many countries of the world. To avoid this loss, always file a Transmittal of New Technology Form before electronically disclosing an invention, and indicate publication is planned.

2. PRINTED MATTER subject to copyright (software, books, certain reports). If this sort of material is distributed without the copyright notice, PNL's right to copyright the material may be lost. PNL does not have the right to copyright material developed under Government funding (our 1830 Contract) without Government permission. DO NOT attach copyright notices to 1830 materials, unless you have received permission to do so.

3. TRADEMARK MATERIAL (words, phrases, graphics). Such marks are unique to a vendor's goods. PNL sells few goods, so we have few trademarks. However, PNL does market a number of software packages with registered trademarks (such as Chernolit and Mepas). A trademark is used as an adjective, -- such as CHERNOLIT software -- set apart from surrounding words with capitalization, italics, or special type.

For intellectual property questions, contact **Steve May (375-2387).**

What Electronic Publishing Services Are Available to Help?

IS&S and Communications together offer a set of services to help organizations make their information available on either the private (PNL-only) or public information space. These services include:

- Information authoring/coding service
- Information management service
- Server setup service.

Information Authoring/Coding Service - This is a range of services such as consultation on how to structure your information to make it more effective electronically, editorial review, and conversion into common Internet formats. Contact **Pam Novak (376-1243)** for more information on this service.

Information Management Service - The Information Management Service allows you to publish your electronic information network-wide without maintaining a server. This service configures, operates, and maintains a server for you. Your information space is implemented and changed according to the your instructions. Costs for this service are the hourly rates to implement or update your information (usually a few minutes per document). Contact **Beth Hetzler (375-6690)** for more information on this service.

Server Setup Service - The Server Setup Service helps customers install their own server to implement their information space. This service provides installation of a standard electronic publishing server configuration, an operations guide, and an approved server security plan. Only labor costs are charged. NOTE: This service is only appropriate for staff who are already familiar with server administration. Otherwise, use the Information Management Service. Contact **Jeff Simmelink (375-2795)** for more information about this service.

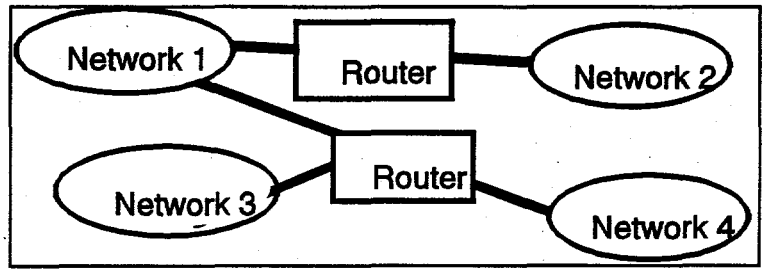
NOTE: These services are implemented using a set of servers running the Gopher+, WWW, and WAIS protocols. Some servers are managed by IS&S and others are managed by users at PNL. The PNL WWW server is managed by Communications. Each information space is supported by the server(s) that contains its data.

ATTACHMENT B

Technology and Issues of Internet Connection

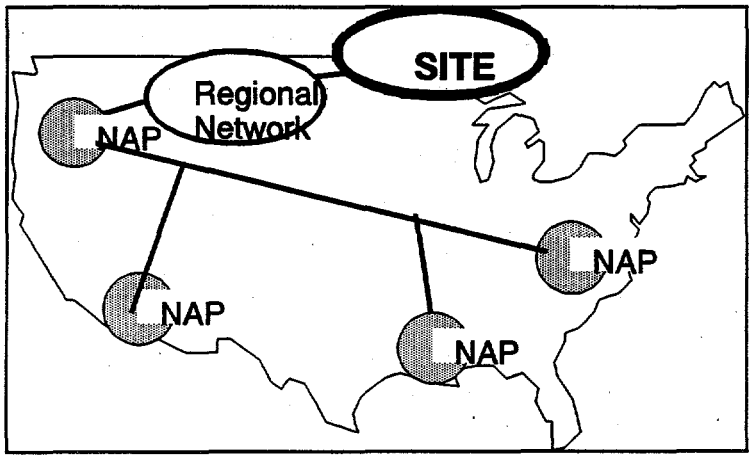
Connecting Networks

Two or more distinct networks are connected using a router, an electronic "traffic cop" that can move data from one network to another as needed. Every network has an address and may be connected to one or more routers.

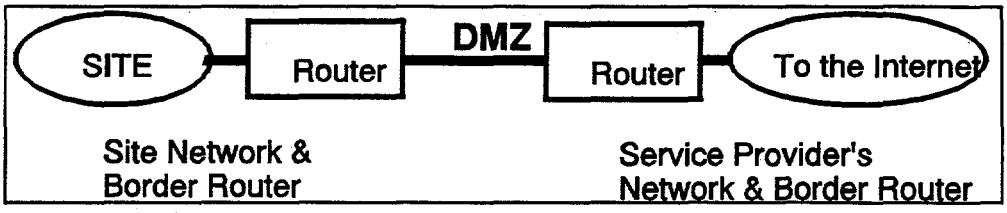


The operators of each interconnected network reach peering agreements that determine how their network may be used to reach other destinations in accordance with their usage policies. Each router is configured to advertise certain reachable networks and not advertise others, in this way the peering agreements are enforced.

To join the Internet a site connects with one or more Internet service providers, either public regional networks (like NorthWestNet) or large private networks (like the Energy Sciences Network, ESnet). In the U.S., these service providers are connected either directly or through peering to National Access Points (NAPs) that are interconnected in a privatized national backbone (the former NSFnet).



When a site and a server provider interconnect the provider puts their router at the site and the site places their own router adjacent to it, each party configures and maintains their own router (and through it protects their interests). The (small) network between these two routers is commonly called a De-Militarized Zone (DMZ).



Security when connecting networks

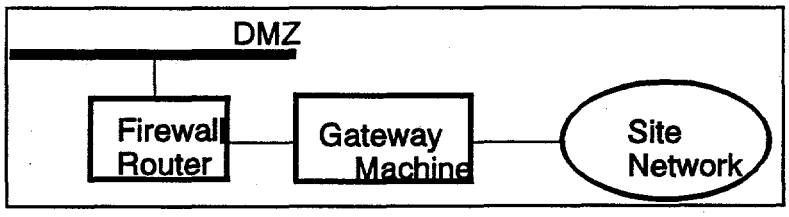
The DMZ can become a security buffer that separates unregulated access from controlled access, this occurs when the site's router is configured as a firewall router. A firewall router limits network traffic according to an analysis of the destination of each piece of Internet traffic passing the router. Security using firewalls rests on protecting the access to information and services.

Evolution of firewall-based security follows a four phase process where each phase builds on the last, represents greater capability from the Internet connection, and demands increased sophistication from the network developers and operators.

Phase 1 Firewall
(Secured Gateway Machines)

In phase 1 a gateway machine is dedicated to providing all internal and external Internet access. The gateway machine is the only machine attached to the firewall.

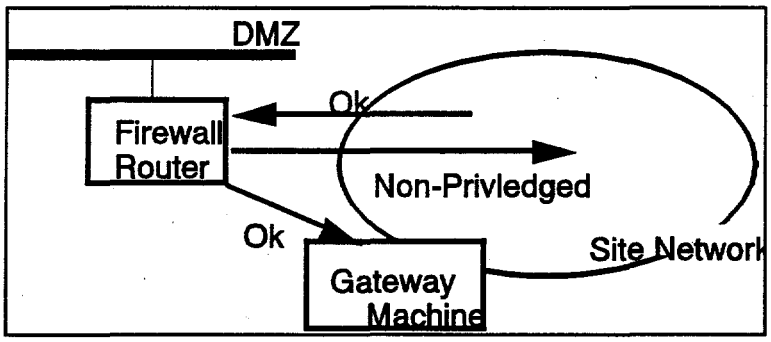
External users access services running on the gateway machine. Internal users must log on to the machine (or access it through some proxy means) and from there access the Internet.



Phase 2 Firewall
(Permeable Firewall, Secured Incoming Services)

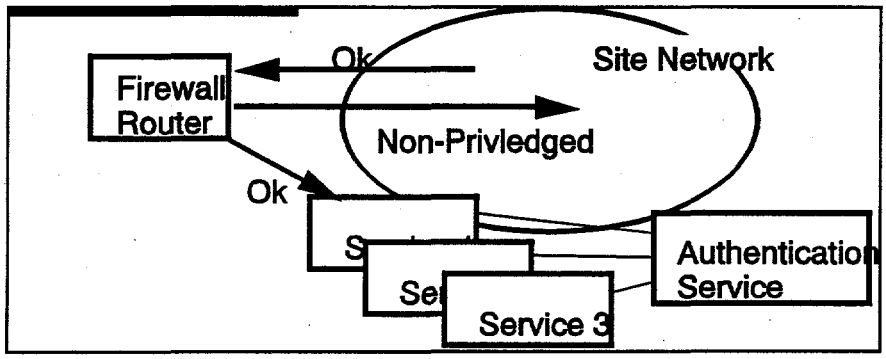
A permeable firewall maintains the advantages of limiting external access to a single trusted machine while allowing internal users full, direct access to the Internet.

The firewall permits the passage of all outgoing traffic without impediment. Incoming traffic is allowed if it goes to non-privledged ports. Incoming traffic to privileges ports is restricted to the gateway machine.



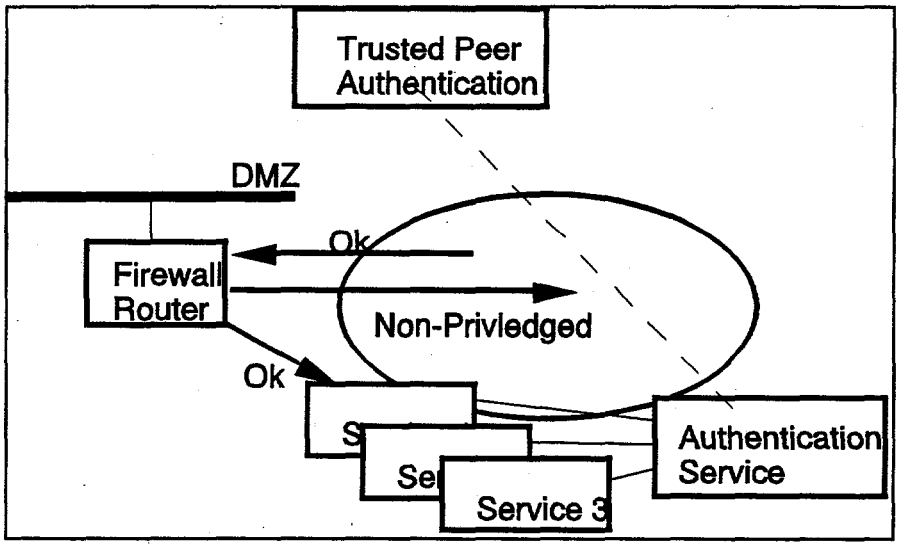
Phase 3 Firewall
(Permeable Firewall, Multiple Secured Incoming Services)

In phase 3 the architecture of a permeable firewall is extended to allow multiple incoming service points, each of which is individually secured. Generally at this phase it becomes necessary to have some sort of trusted authentication scheme so that each external service machine can authenticate an external user as needed - the alternative is to maintain many redundant authentication services.



Phase 4 Firewall
(Permeable Firewall, Multiple Secured Incoming Services, Distributed Trust)

In phase 4 authentication trust can be distributed to external peers, removing the need to locally authenticate every potential external Internet user. Kerberos is the technology of choice for distributed authentication and allows two (or more) sites to establish mutual authentication trust.



Current Interconnection Practice

The Hanford Site internal network is administered and implemented as a collection of many smaller networks, as is customary and required. At the highest level these networks are grouped into two large sets that we will label as HLAN (the Hanford Local Area Network) and PNLnet (The PNL network). Historically, these two collections have been referred to jointly as HLAN, but the distinction is important here.

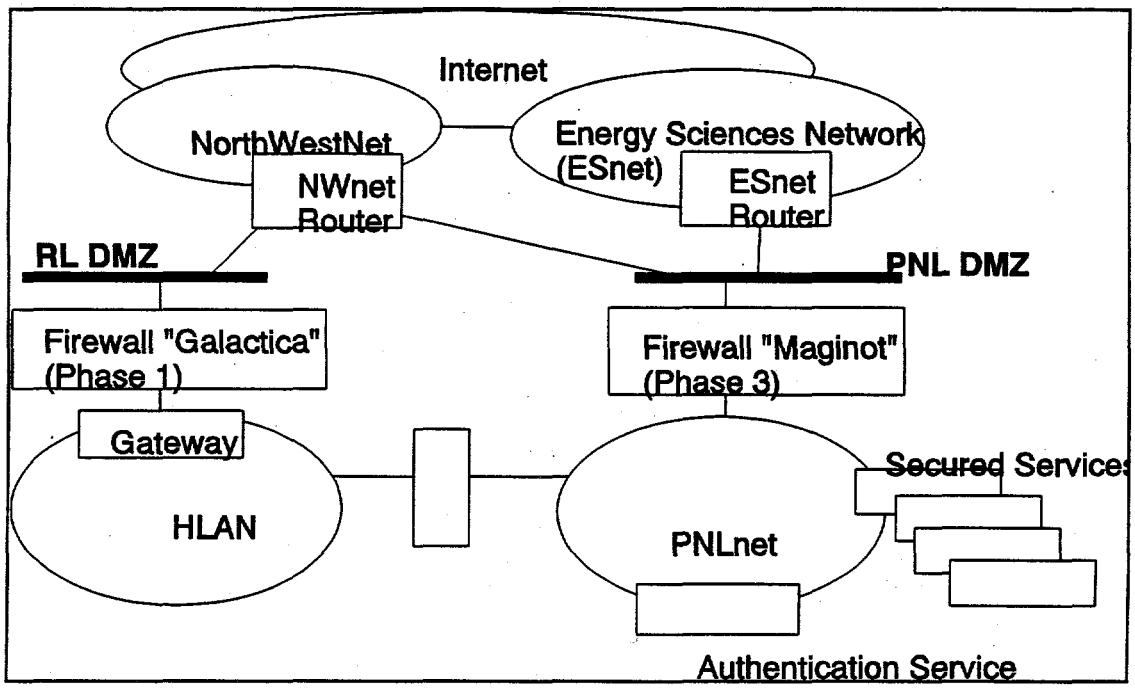
The bulk of HLAN is connected to the Internet through the NorthWestNet regional service provider. A firewall is employed using the "Phase 1" strategy (i.e., all access in or out is through a gateway machine). An agreement has been reached with the Energy Sciences Network (ESnet) to carry all Hanford traffic but this option has not been implemented.

The PNL portion on HLAN (PNLnet) is connected to the Internet through both the Energy Sciences network (ESnet) and NorthWestNet. PNL employs a "Phase 3" permeable firewall that allows internal staff full access to the Internet and limits Internet access to PNLnet to a select set of services. A smartcard-based authentication scheme is in place and implemented with an internally-developed authentication server (SIDNEY - Secure ID Server).

These two Site networks are interconnected by a router that allows the free exchange of traffic between them. This interconnecting router does not allow any access to or from the Internet through it.

The next diagram captures the essence of the Hanford Site's current Internet connectivity. The true implementation of Hanford's networks is much more complex than depicted here. There are two service providers (ESnet and NWnet), two major DMZs, and two firewall routers shown. The firewall implementation within HLAN is through a gateway machine, a Phase 1 implementation. The firewall implementation within PNLnet is through a permeable firewall router to multiple secured services, a Phase 3 implementation.

The Site contractors are each exploring advancing their firewall implementation to the next phase of capability.



Interconnection Technology Summary

The problems of connecting with the Internet and maintaining adequate access controls are well understood and routinely solved. The use of firewalls as a mechanism for access control has been a frequent practice throughout the Internet, and its use is becoming common practice as sites respond to an increasingly more open Internet.

The implementation of access control differs between the contractors, as a natural outgrowth of historically differing needs. We all continue to refine our implementations of access control and have no plans to remove the firewalls until alternate, adequate, or superior methods become available.

The planning of network-based services must always be sensitive to the network interconnection environment, the types of security protection the firewall offers (and what it does not), and the functional capabilities of the network.

Most commercial or public domain firewall packages are now based on some form of Proxy server technology. There is currently an Internet Inter-Engineering Task Force (IETF) working on Internet gateway security systems. The initial IETF draft document is based on SOCKS protocol, which is becoming an industry standard. These systems all allow internal users to access the Internet in a user friendly way but also gives management full control over access.