
GUIDANCE FOR PROVIDING INFORMATION TO THE PUBLIC VIA PUBLIC ACCESS SERVERS



November 1995
Revised June 1998

U.S. Department of Energy
Assistant Secretary for Human Resources and Administration
Deputy Assistant Secretary for Information Management
Office of Information Management

U.S. DEPARTMENT OF ENERGY FOR PROVIDING INFORMATION TO THE PUBLIC VIA
PUBLIC ACCESS SERVERS

TABLE OF CONTENTS

| | |
|---|-----|
| EXECUTIVE SUMMARY | iii |
| BACKGROUND | 1 |
| SCOPE | 1 |
| GENERAL GUIDANCE | 2 |
| Presentation | 3 |
| Text | 3 |
| Graphics | 3 |
| ROLES AND RESPONSIBILITIES | 3 |
| DETERMINING IF INFORMATION IS APPROPRIATE FOR PUBLIC POSTING | 3 |
| POSTING SENSITIVE UNCLASSIFIED INFORMATION | 4 |
| TYPES OF PUBLIC ACCESS SERVERS | 6 |
| Electronic Bulletin Boards (BBSs) | 6 |
| FTP Servers | 6 |
| Gopher Servers | 6 |
| World Wide Web (Home Pages) | 7 |
| REFERENCES | 8 |

U.S. DEPARTMENT OF ENERGY GUIDANCE FOR PROVIDING INFORMATION TO THE PUBLIC VIA PUBLIC ACCESS SERVERS

EXECUTIVE SUMMARY

The U.S. Department of Energy inherently accepts a certain level of responsibility associated with providing unclassified information to the public via public access servers or PAS. Many issues need to be addressed prior to the actual posting of information to a PAS. A determination and management approval should be granted prior to establishing a PAS, posting information on a PAS, and providing maintenance for the PAS as well as the information presented via the PAS. Many alternatives for posting unclassified information to the public are available. Electronic bulletin boards (BBSs), gopher servers, ftp servers and, WWW servers (home pages) are popular today.

These general guidances should be followed for establishing any type of PAS:

- ▶ The PAS should reside on a system dedicated solely to information distribution, and only information to be distributed should reside on the system.
- ▶ Servers should run with as little privilege as necessary.
- ▶ Whenever possible, server software should be executed in a restricted file space
- ▶ System administrators should closely monitor the integrity of the system and the information to be distributed.

The task of providing information to the public via public access servers requires the involvement of at least the following elements of an organization: *management; system (network) administrators; information contributors; developers; and, maintainers.*

Management should be aware of and approve any ongoing activities associated with establishing and maintaining a PAS and the posting of information from his/her organization to that, or any other PAS. (System (Network) Administrators are the individuals responsible for the network where the PAS resides.) Information Contributors are the individuals who provide information in electronic format to be made available on a PAS. Developers are responsible for establishing a PAS for an organization. Maintainers are responsible for keeping the PAS public interface (e.g., a WWW home page) "up and running," as well as adding, modifying or deleting information as required.

The following steps should be used to determine if information is suitable for posting on a PAS:

- . Determine if the information is classified. If the information is classified, it **can not** be posted to a PAS.
- . Determine if the information is sensitive unclassified.
- . Review the information and determine if an actual benefit could be derived by the public from the posting of the information on a PAS. Do not post information just for the sake of posting it.
- . The posting organization's manager (usually the information's owner), should review the information to ensure that the information doesn't provide misinformation or information that could potentially bring embarrassment to the Department.
- . Information still qualified for posting to a PAS should be presented in conformance with the same standards that are used in the preparation of "hard copy" versions of the same information, where applicable.

Commercial Off The Shelf (COTS) Software applications or tools can only be made available to the public via a PAS **if there are no software licensing violations in doing so.**

In some instances, it may be appropriate information to post to a PAS that is found to be sensitive unclassified. However, if the information is sensitive due to the confidentiality of it's contents, then the information **may not** be posted.

**U.S. DEPARTMENT OF ENERGY
GUIDANCE FOR PROVIDING INFORMATION TO THE PUBLIC
VIA PUBLIC ACCESS SERVERS**

BACKGROUND

The Department of Energy's "Openness Initiative" is further enabled through posting unclassified Departmental information on public access servers (PASs). These PASs should be used for official business only. DOE inherently accepts a certain level of responsibility associated with the activities undertaken in order to provide this service to the public.

Many issues need to be addressed prior to the actual posting of information to a PAS. Certain questions arise relating to:

- What information should an organization make available to the public electronically?
- What method should the organization adopt for providing access to this information (ftp, gopher, WWW, BBS, etc.)?
- Where will the system used to provide the information be located (both physically and in regard to the LAN's configuration scheme)?
- Will management approve the procurement of a new system or re-allocation of an existing system?
- What is going to be the policy of the data owner's organization on periodic updates and reviews of the relevance of the information made available to the public?

Once the information has been approved for posting to a PAS, the means of posting also needs to be reviewed and approved. Will the information be posted to an anonymous ftp site, a gopher server, or linked to a WWW home page? Organizations should develop standards for their site incorporating guidance presented in this document.

Numerous alternatives for providing the public electronic access to unclassified information are available to the Department. Electronic bulletin boards (BBSs) have been a longstanding means of accomplishing this. Today, with the increased exposure to the Internet by an ever increasing number of DOE and DOE-contractor personnel, many departmental organizations have taken advantage of some newer techniques like the World Wide Web (WWW) - specifically, WWW "home pages."

SCOPE

This guidance will identify suggested steps to take in determining if information is indeed, destined for public consumption; and if so, what steps should be taken in its posting to ensure the integrity and availability of the information. Additionally, this guidance will identify alternative methods of providing information to the public and discuss the benefits and disadvantages associated with each. Suggested standards will also be addressed, with respect to information presentation and PAS maintenance.

GENERAL GUIDANCE

Information should never be posted to PASs simply because they are there. The DOE discourages the posting of trivial information that will only contribute to the degradation of service (with respect to the Internet and PASs). While it may seem that posting information on your organization's home page is simple to do initially, certain consequences should be made known before they occur. The more information that is posted to PASs, the greater the demand for periodic maintenance on that PAS. The system owner will be charged with ensuring that only approved information is made available, that the information has maintained its integrity (i.e., accuracy), and, if required, that appropriate contingency plans have been prepared to ensure its availability. It should also be noted that information posted to public access services is considered an official record, thus a review process is necessary. Posted information also needs to be reviewed to determine if it's still necessary to be posted. Remember, the information is taking up storage space on the PAS and if that information is in graphic form, it's taking up a lot of storage space. The greater an organization's commitment to posting information on PASs, the greater the commitment must be to provide personnel to spend more time performing periodic maintenance on and upgrades to the PAS.

Some examples of information that should generally be deemed inappropriate for posting to public access servers are: information system security plans; information system security vulnerabilities; and, other information system security-related information. Other types of information that should be deemed inappropriate also include: licensed software; administrative information such as financial, proprietary, and CRADA¹; and Unclassified Controlled Nuclear Information.

To help mitigate vulnerabilities, these general guidances should be followed for establishing any type of PAS:

- ▶ The PAS should reside on a system dedicated solely to information distribution, and only information to be distributed should reside on the system. Assume that any information placed on the system will be available to the Internet public, should the server software be compromised.
- ▶ Servers should run with as little privilege as necessary. If at all possible, server software should not run as "root," thus limiting possible damage if an intruder discovers a vulnerability.
- ▶ Whenever possible, server software should be executed in a restricted file space (*chroot* environment in Unix), thus restricting files to which the server has access and making it more difficult for users to access unintended information.
- ▶ System¹ administrators should closely monitor the integrity of the system and the information to be distributed. Cryptographic "checksum" utilities, such as SPI and Tripwire, can create system snapshots and notify administrators of unauthorized modifications.

¹ CRADA - Cooperative Research and Development Agreement information that pertains directly to the CRADA agreement itself. General information describing the planned research and development between the DOE-element and other parties to the CRADA may be appropriate for posting to public access servers.

Presentation

Text

Departmental information presented on PASs should conform to the same standards that are currently used when an organization provides "hard copy" versions of reports, documentation, studies, etc. to its customers.

Graphics

The use of graphics in the posting of information to PASs should be kept to a minimum because graphics require:

- An enormous amount of storage space;
- Much longer transfer times (i.e., takes much longer to transfer to a viewing client, than text); and,
- Sophisticated hardware and software in order for the user to view remotely.

Use of graphics for organizational logos is not discouraged; however, these logos should not appear on every iteration of information posted to their PAS. Graphics are also appropriate in displaying scientific, budgetary, and statistical information.

Graphics may seem the way to entice the public to your PAS, but due to the long transfer times associated with each graphic, too many graphics will likely discourage public visits to your PAS.

ROLES AND RESPONSIBILITIES

The task of providing information to the public via public access servers requires the involvement of at least the following elements of an organization: *management; system administrators; information contributors; developers; and, maintainers.*

Management. Management should be aware of and approve any ongoing activities associated with establishing and maintaining a PAS and the posting of information from his/her organization to that, or any other PAS.

System Administrators. System (Network) Administrators are the individuals responsible for the network where the PAS resides. The establishment of a PAS should be coordinated with the system administrator for the network where the PAS will reside. Periodic back-ups should be made to ensure availability and integrity of the information.

Information Contributors. Information Contributors are the individuals who provide information in electronic format to be made available on a PAS. Information Contributors are responsible for ensuring that the information in electronic format is a true, complete representation of its original content, even when undergoing changes in form or storage medium. Information Contributors are also responsible for verifying the correctness (content, spelling and grammar) of the information.

Developers. Developers are responsible for establishing a PAS for an organization and working with that organization to achieve the design and functionality being sought.

Maintainers. Maintainers are responsible for keeping the PAS public interface (e.g., a WWW home page) "up and running," as well as adding, modifying or deleting information as required.

DETERMINING IF INFORMATION IS APPROPRIATE FOR PUBLIC POSTING

Prior to posting any information on a PAS:

1. Determine if the information is classified. If the information is classified, it **can not** be posted to a PAS.

2. Determine if the information is sensitive unclassified.
 - ◆ If the information is sensitive unclassified, it can only be *considered* for posting to a PAS **if**: the information is determined to be sensitive unclassified due to integrity or availability protection attributes.
 - ◆ **If there is a need to protect the confidentiality (i.e., prevent unauthorized disclosure) of the information, then it is clearly *not* a candidate for posting to a PAS.**
3. Review the information and determine if an actual benefit could be derived by the public from the posting of the information on a PAS. Do not post trivial information just for the sake of posting it.
4. The posting organization's manager (presumably the information's owner), should review the information to ensure that the information doesn't provide misinformation or information that could potentially bring embarrassment to the Department.
 - Misinformation is erroneous information (e.g., wrong quarterly fuel consumption projections). If the information provides misinformation, it **can not** be posted to a PAS.
 - Information that could potentially bring embarrassment to the Department is information that portrays an organization (the information's owner) and the Department in an unacceptable light (e.g., racist, harassing, belligerent, or offensive information, as well as factual, yet unpopular information). If the information could potentially bring embarrassment to the DOE, it should be referred to management for approval.
5. Information still qualified for posting to a PAS should be presented in conformance with the same standards that are used in the preparation of "hard copy" versions of the same information, where applicable. Some information may not be of a format that is conducive for equating its presentation to a "hard copy" version.

If the information is presented in a suitable manner and in conformance with "hard copy" standards (if applicable) then the information may be posted to a PAS.
6. Commercial Off The Shelf (COTS) Software applications or tools can only be made available to the public via a PAS **if there are no software licensing violations in doing so**. Organization's wishing to post proprietary software developed "in-house" should seek management approval for posting to a PAS. The majority of the software that will meet this condition is anticipated to be that which has been developed by DOE's laboratories.

If the posting, or subsequent downloading, of information (in this case software) will not violate any associated software licensing agreements and has been granted management approval, then the information may be posted to a PAS. If the approved information is "Shareware," than be sure to include the accompanying notice conveying copyright and the request for royalties being paid to the Shareware developer.

POSTING SENSITIVE UNCLASSIFIED INFORMATION

In some instances, it may be appropriate to post to PASs information that is found to be sensitive unclassified. If the information is sensitive due to the **confidentiality** of it's contents, then the information **may not** be posted. Integrity and availability are the other two protection attributes used to determine if information is sensitive unclassified.

If an organization has the responsibility to provide information to the public in a predetermined timely manner, the degree of tolerance

for the unavailability of that information is very low. Therefore, adequate protections must be in place to ensure a reasonable level of assurance that the PAS used to provide the public the information will be maintained at a high state of readiness. This requirement may necessitate the creation and testing of a contingency plan for ensuring timely **availability**. [For guidance in the area of contingency planning, see the DOE guidance, "*Disaster Recovery Program Guidance*," dated July, 1991.]

An organization may also demand that reasonable precautions are exercised to provide an assurance that the information posted to a PAS is free of errors and is maintained in the same condition, and that modification or delete capabilities are restricted from the public's execution. In this case, **integrity** is the concern which deems this information sensitive unclassified, thus requiring certain protection measures.

TYPES OF PUBLIC ACCESS SERVERS

A PAS is used in this guidance generically to categorize any means used to provide (post) information that is intended to be accessed by the public in an anonymous manner.

Many alternatives for posting unclassified information to the public are available. Electronic bulletin boards (BBSs), gopher servers, ftp servers and, WWW servers (home pages) are popular today.

Electronic Bulletin Boards (BBSs)

Electronic Bulletin Boards were very popular prior to the proliferation of the Internet. Instead of accessing this type of PAS via the Internet, remote users need to have a modem and communications software and connect directly with the BBS host. BBSs typically provide the following services: teleconferencing, electronic mail, forums, and most often, some library or libraries of files that could be viewed and/or downloaded by the remote user. These files could be data or software. While still in use today, the non-graphical user interface of most BBSs have caused somewhat of a decline in popularity for this form of PAS.

Among the potential security vulnerabilities exhibited by electronic bulletin boards, the following relate to the information available from this type of PAS:

- ▶ Users may alter or delete information or software.
- ▶ People may connect to a BBS host and use writable areas of a BBS file system to exchange files. This is a popular technique used by people to trade copyrighted software and pornographic pictures.
- ▶ Configuration errors may permit unintended access to sensitive files.

FTP Servers

The File Transfer Protocol, or FTP, is the basis for the oldest and most common type of PAS on the Internet, the anonymous FTP server. Anonymous FTP servers allow unauthenticated access to a portion of a host's file system. The server software allows remote users to retrieve files and occasionally it allows file uploads or even more advanced operations, such as index searches and file compression depending on the manner in which the server is configured.

Among the potential security vulnerabilities exhibited by anonymous FTP servers, the following relate to the information available from this type of PAS:

- ▶ Users may alter or delete information or software.
- ▶ People on the Internet may use writable areas of an FTP file system to exchange files. This is another popular technique used by people to trade copyrighted software and pornographic pictures.
- ▶ Configuration errors may permit unintended access to sensitive files. For example, a common mistake when setting up an anonymous FTP server is to make a copy of the system password file in the area available to remote users. If any local users have chosen weak passwords, intruders may then use this password file to break into the system.

Gopher Servers

Gopher servers are newer to the Internet than FTP servers. Gopher servers have several advantages over the FTP servers. These include:

- ▶ Gopher servers provide greater flexibility in the types of information that can be distributed. The information returned to remote users can include links to information sources at other Internet sites, gateways to other types of services (e.g., FTP and Telnet servers), and even dynamic information generated by local software and driven by remote user requests.

- ▶ Gopher servers are easier to use than FTP servers. Most client software includes some sort of the graphical user interface and it usually knows how to handle different types of files that a user retrieves. For example, a typical program will automatically run a display program when a graphic image is retrieved.

However, these advantages, combined with the relatively new development stage of the software, create the potential for increased risk to the machines and associated systems running gopher software.

Among the potential security vulnerabilities exhibited by gopher servers, the following relate to the information available from this type of PAS:

- ▶ Under some circumstances, remote users can trick the gopher server into retrieving any file on the system, including sensitive system files.
- ▶ Remote users can possibly cause the gopher server to execute arbitrary, undesired shell commands. Sometimes, gopher servers are configured to execute programs on the server host; they will then pass user-specified arguments to the program on the command line. On some systems, the configuration of these arguments will cause additional programs to be executed.

World Wide Web (Home Pages)

The most recent development on the Internet is the astonishing proliferation of World Wide Web (WWW) information servers. These servers offer many advantages, including:

- ▶ WWW documents allow access via hypertext to thousands of information sources and large amounts of data from around the world.
- ▶ WWW browsers such as NCSA Mosaic are graphical and easy to use.

These advantages have helped the WWW become the fastest growing information service on the Internet. However, these advantages--in similar fashion to those of gopher servers--combined with the new and untested nature of the server software, introduce the potential for compromise of the server and the information contained on it.

Among the potential security vulnerabilities exhibited by WWW servers, the following relate to the information available from this type of PAS:

- ▶ The server may allow access to files located outside the file area designated for WWW access. Intruders may be able to trick some HTTP (HyperText Transfer Protocol) servers into returning system files.
- ▶ Most HTTP servers support executable scripts (Common Gateway Interface, or CGI, scripts) that compute information to be sent back to remote users at the time of demand. This is the area of greatest vulnerability for an HTTP server. The system often cues these scripts using input from the remote users; this information is generally supplied via a fill-out form. If these scripts are not carefully written, intruders can subvert the scripts to execute arbitrary commands on the server system.

REFERENCES

The author used the references listed below to develop the information contained in this document:

1. CIAC-2308 R.2, "*Securing Internet Information Servers*," December, 1994 (.pdf and html versions)
2. CIAC- 2307, "*Electronic Resources for Security Related Information*" (.pdf version)
3. CIAC-2317, "*Windows NT Managers Guide*" (.pdf version)

note: The URL is: <http://ciac.llnl.gov/cig-bin/index/documents>