

Network Working Group
Request for Comments: 1355
FYI: 15

J. Curran
NNSC
A. Marine
SRI
August 1992

Privacy and Accuracy Issues in Network Information Center Databases

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard. Distribution of this memo is unlimited.

Abstract

This document provides a set of guidelines for the administration and operation of public Network Information Center (NIC) databases. The purpose is to formalize procedures for the responsible handling of the personal and organizational information maintained by NICs in publically accessible databases, and to improve the accuracy and accessibility of such data where appropriate.

Acknowledgments

This document is based upon the work of the Network Information Services Infrastructure (NISI) working group in the User Services Area of the IETF. Thanks are due to the members of this working group who contributed ideas and comments, especially to Glee Cady (University of Michigan) for her significant contributions. Special thanks are also extended to Steve Crocker (TIS) for his guidance in this area. Due to the natural overlap between NIC databases and public user directories, this document also references concepts contained in the North American Directory Forum's (NADF) "User Bill of Rights for Entries and Listings in the Public Directory" (RFC 1295).

1. Purpose

The purpose of this document is to consider the privacy and accuracy issues that result from many NIC databases being publicly accessible. This document considers only generic concerns about such systems; it intentionally does not make recommendations for specific databases on the Internet. Clearly, it is the responsibility of each NIC to determine what procedures should apply for each of its databases. The document discusses the obligations a NIC that maintains such a

database has towards those about whom data appears in the database. These obligations apply to database entries that contain information that is publically accessible to Internet users.

2. Background and Organization

In fulfilling the functions of a Network Information Center, each NIC needs to collect and distribute a variety of information about the network it serves. Much of the information handled by a NIC is "directory" information that provides pointers to people, organizations, and resources throughout a network. The use of publically accessible databases to disseminate such data is seen as beneficial to the Internet because it allows efficient information retrieval by users, Network Operation Centers (NOCs), and other NICs.

This document is organized into two parts. The first part contains recommendations for preventing unauthorized disclosure of information in NIC databases. The second part recommends formal accuracy guidelines for NIC databases.

3. NIC Database Privacy

The existence of publically accessible databases brings up a number of significant questions regarding controls over the gathering and distribution of the data. It is important that these concerns are addressed prior to the wide-scale deployment of a public NIC database or a NIC risks having to retrofit an established system to formal guidelines regarding such controls when they are finally available.

For each publically accessible database that a NIC manages, the NIC needs to provide a clear statement of the purpose of the database, the types of information it contains, and the privacy policy that applies to the information stored within it. In general, this policy should inform people or organizations listed in the database of the content and purpose of their database entries. Specifically, the privacy policy should:

- 1) Describe why the NIC needs the information and how it will use the information.
- 2) List of all the information being stored in an entry.
- 3) Detail which information will be made available outside of the NIC, to whom it will be made available, and for what purpose.
- 4) Provide for notification of any person or organization added to the database at the request of a third party.

- 5) Explain how to have the information changed or updated.
- 6) Explain how to get information removed from the database, including any references to one's information in another's database entry.
- 7) Explain the consequences of removing information from the database and of failing to provide all or part of the information a NIC requests.

The privacy policy enables people to make informed decisions regarding which information to supply for a given NIC database. Any information supplied should be treated in a manner consistent with the current privacy policy. If a NIC makes a database available in its entirety to another organization, the NIC should also provide that organization with a copy of the current privacy policy for the database.

4. NIC Database Accuracy

The value of any NIC database is dependent on the accuracy and timeliness of its contents. Any database not being maintained well can create major difficulties for those using it and for those people and organizations listed.

For each publically accessible database that a NIC operates, the NIC should have a clear statement that describes the process that the NIC uses to maintain accuracy in the database. This statement could be combined with the privacy statement described above for sake of administrative convenience.

The accuracy statement informs potential participants in the database of the precautions taken by the NIC to ensure accurate information. Any information supplied should be treated in a manner consistent with the current accuracy policy. If a NIC makes a database available in its entirety to another organization, the NIC should also provide that organization with a copy of the current accuracy policy for the database.

The accuracy statement should:

- 1) Allow an individual or organization access to its own database entry, including private fields, for the purpose of correcting errors.
- 2) Allow an individual or organization to correct any errors that occur in its database entry.

- 3) Inform an individual or organization when information about them appears in an entry belonging to another party, so that the individual or organization can review that information and have the opportunity to submit corrections.
- 4) Change information in an entry only at the request of or with the approval of the individual or organization about which the entry applies.
- 5) Encourage an individual or organization to report any errors that occur in the database entries of others.
- 6) Provide for a "date of last review" for each entry in the database; this would reflect the date that the entry was last checked by the owner for accuracy.
- 7) Describe any and all practices used by the NIC to confirm data prior to inclusion in the database.
- 8) State the data backup procedures in use for this database.

5. Security Considerations

This memo briefly considers the security aspects of information in NIC databases. This memo should be revisited as security infrastructure becomes more developed in the Internet.

6. Authors' Addresses

John Curran
NSF Network Service Center (NNSC)
10 Moulton Street
Cambridge, MA 02138

Phone: (617) 873-3400
Email: jcurran@nnsf.net

April N. Marine
SRI International
Network Information Systems Center
333 Ravenswood Avenue, EJ294
Menlo Park, CA 94025-3493

Phone: (415) 859-5318
Email: april@nisc.sri.com