CENDI / 2000-1

CENDI

CENDI GUIDELINES FOR PRIVACY OF CUSTOMER INFORMATION

Submitted by
CENDI IT Security Working Group

Prepared by
Gail Hodge
Information International Associates, Inc.
Oak Ridge, Tennessee

August 2000

TABLE OF CONTENTS

CENDI IT Security Working Group Members

Al Astley, Co-chair (DTIC)

Simon Chung (NASA)

Dan Carrigan (NAIC)

John DiDuro (NTIS)

Gail Hodge (CENDI Secretariat)

Mark Silverman, Co-chair (NLM)

Richard Thompson (NAL)

CENDI is an interagency cooperative organization composed of the scientific and technical information (STI) managers from the Departments of Agriculture, Commerce, Energy, Education, Defense, the Environmental Protection Agency, Health and Human Services, Interior, and the National Aeronautics and Space Administration (NASA).

CENDI's mission is to help improve the productivity of Federal science- and technology-based programs through the development and management of effective scientific and technical information support systems. In fulfilling its mission, CENDI member agencies play an important role in helping to strengthen U.S. competitiveness and address science- and technology-based national priorities.

Forward

Increasingly, staff of CENDI agencies, both in Information Technology (IT) and in other positions within the agencies, have access to or are involved in the processing of private information from the public and other customer groups. Much of this information is coming from increased use of telecommunications such as e-mail, the Internet and the Web. The information may involve private information such as addresses and phone numbers, or proprietary information such as the subject content of a search. At the same time, there is increased concern among the government and the public about privacy related to such information.

The CENDI IT Security Working Group was formed at the Annual Planning Meeting in August 1999. It was officially chartered in November 1999. After several initial discussions about various IT issues of concern to the agencies, the group decided to focus on the issues surrounding the Web and customer information. It was determined that one of the problems is that staff, both within IT and outside IT, currently have inadequate awareness training in issues surrounding this type of information in this environment. The aim of this document is to act as a basic awareness document for all levels of staff. CENDI agencies that accept this are encouraged to modify it, extend it, or include it in other mission-specific procedures and training materials.

1.0 BASIC PREMISE OF PRIVACY IN PUBLIC INFORMATION

Access to all kinds of information is increasingly available and pervasive at all levels of the agencies. More information is being declassified as policies dictate. More information is being created every day. Agency staff have increased contacts with customers and other staff members via e-mail, which provides a documented record of the "conversation" that can be easily sent to other individuals both within and outside the agency.

Under these conditions, the first premise of IT Privacy is

YOU DON'T LOOK JUST BECAUSE YOU CAN AND YOU DON'T DIVULGE WHAT YOU SEE UNLESS REQUIRED TO DO SO IN THE PERFORMANCE OF YOUR JOB.

2.0 STAFF AWARENESS

GUIDELINE: *Agencies should provide training to staff who, in the course of their duties, will handle user information so that they understand this is a sensitive issue. Rules of disclosure apply to electronic as well as to other media of communication.*

3.0 GENERAL

In the past, many interactions between customers and the agencies were through systems that required some level of registration. As registration requirements are eliminated, users may expect that their access through anonymous channels, such as gopher, ftp and web, automatically results in all information being anonymous.

GUIDELINE: *Users who are accessing a system through anonymous means must be made aware of cases where their information will not be anonymous. It is recommended that every system have a banner that states there should be no expectation of privacy.*

The remainder of this document gives specific guidance related to the Web, Listservs, and other electronic communications with customers. These guidelines are extending the Privacy Policies on a Federal Web Site memo from the Office of Management and Budget (OMB).

4.0 LOGS

4.1 E-mail Logs

For back-up and recovery purposes, agencies keep logs of e-mail messages s received and sent.

GUIDELINE: *These should be kept only as long as necessary.*

4.2 Application Logs

Program logs (web server logs, anonymous ftp logs, etc.) can provide information about what a user looks at and searches for, and even application click and navigation histories. Some sites may publish statistics derived from their log files, making this information available to the general public.

GUIDELINE: *Log information should be treated as sensitive and protected against accidental disclosure. This is the equivalent of traditional library records. Log data should only be disclosed for official government use, including law enforcement, when investigating computer security and/or national security incidents.*

GUIDELINE: *The decision to publish statistics must be determined by the individual agency's mission and policies. The presentation of statistics should not allow for identification of a single computer, individual name, or individual non-government institution.*

5.0 WEB-BASED TRANSACTIONS AND OTHER APPLICATIONS

In addition to logs of Web activity, private information can be collected from the Web via web forms, cookies, and other applications.

GUIDELINE: *Users should be told in advance as close to the main entry point for the application as possible, that information is being collected and the purpose of the collection. The agency must disclose (in accordance with the June 2, 1999, memo from OMB) any information that is left or collected surreptitiously by a client (e.g., browser).*

6.0 LISTSERVS, NEWSGROUPS, BULLETIN BOARDS

Access to information about the membership of a listserv not only provides access to the list members' e-mail addresses but some level of information about their interests. Listservs can also be used maliciously, resulting in "spamming", or the mass e-mailing of unwanted or inappropriate material.

Most listserv programs have a "Who"-like command that will display the members of the list. Some lists have archives of postings made to the list.

GUIDELINE: *Listserv, newsgroup, and bulletin board subscribers should be made aware of the agency's privacy policy and of the privacy policy of the specific list. This includes what happens to the postings, who has access to the members' e-mail addresses, what is archived, who has access to the archive, and whether or not the archive is available on the Web (which means that it may be indexed by search engines). This information must be presented in the list's welcome message, along with instructions for immediately unsubscribing from the list (if the user does not agree with the list's policies).*

GUIDELINE: *Lists should generally have the "Who" command turned off. However, if there is a reason why the "who" command must be enabled, the list welcome message must include a statement indicating that the list e-mail addresses (e.g., membership) are available to the public.*

GUIDELINE: *The list's welcome message should also contain a statement indicating that the individual subscriber is responsible for the content of his/her messages. The message should indicate that the agency cannot control downstream dissemination of the user's messages and it should suggest that users state in the Subject Line or at the top of the message if they would like to have the information disseminated, limited, or if they request acknowledgement for the content.*

7.0 OFFICIAL GOVERNMENT E-MAIL FROM THE PUBLIC

More and more, transactions between the government and its constituencies will be performed via e-mail. There are policies and guidelines in place that are required by a system of record, by the Privacy Act, and by agency e-mail policies. However, there are some general ethical considerations.

GUIDELINE: *The content of an e-mail message should not be distributed beyond the logical chain required to deal with the message's content. It is important that the employee consider that the communications are from a public source and are part of official government business. If the employee does not know what to do with a particular message, the message should be sent along the official channels, forwarded to others with either implicit or explicit permission from the originator, or deleted. E-mail received in error, captured (i.e., with intrusion detection or virus scanning software) or stumbled upon, should also be treated in the same manner as above.*

GUIDELINE: *Agencies should develop policies on how to handle e-mails that are misdirected and the proper path for handling legitimate inquiries.*