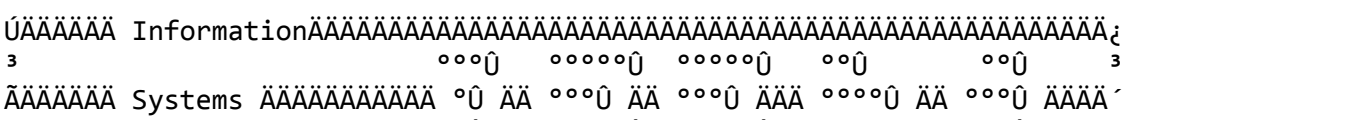

Dedicated to the pursuit of security awareness.....

Volume 3 Number 3 July 1993

IN THIS ISSUE

The ISSM is a quarterly publication of the Department of Treasury, Bureau of the Public Debt, AIS Security Branch, 200 3rd Street, Parkersburg, WV 26101 (304) 480-6355

Editors: Ed Alesius
Kim Clancy
Mary Clark
Jim Heikkinen
Joe Kordella

```
******************************
*                            *
*  WHO'S READING YOUR SCREEN  *
*    by Philip Elmer-Dewitt   *
*                            *
******************************
```

It's a situation that arises a million times a day in offices around the world. An employee has something personal to tell a co-worker---a confidence, a joke, a bit of gossip that might give offense if it were overheard. Rather than pick up the phone or wander down the hall, he or she simply types a message on a desktop computer terminal and sends it as electronic mail. The assumption is that anything sent by E-mail is as private---if not more so---than a phone call or a face-to-face meeting.

That assumption, unfortunately, is wrong. Although it is illegal in some states for an employer to eavesdrop on private conversations or telephone calls---even if they take place on a company-owned phone==there are no clear rules governing electronic mail. In fact, the question of how private E-mail should be has emerged as one of the stickiest legal issues of the electronic age, one that seems to evoke very different responses depending on whose electronic mail system is being used and who is reading the E-mail.

Does the White House, for example have the right to destroy electronic messages created in the course of running the government? That issue came to a head last week when a federal judge barred the BushAdministration from erasing computer tapes containing E-mail dating back to the Reagan era---including electronic memos that are relevant to Iran-contra and might implicate officials in the Iraqgate and Clinton passport scandals.

The White House had issued guidelines that would have allowed staff members to delete that mountain of electronic evidence. Judge Charles Richey dismissed those instructions as "capricious" and "contrary to the law." He specifically rejected the argument that all substantive E-mail had been saved in computer printouts. The paper versions, Richey noted, omit who received the documents and when. "What government officials knew and when they knew it has been a key question in not only the Iran-contra investigation but also in the Watergate matter."

Many historians and legal experts applauded the decision. Government officials, they argue, are civil servants conducting the public's business; the public has the right to review any documents they create--paper or electronic. But how would those citizens feel if it were their E-mail that was being preserved for posterity? Shoudn't private missives sent over a privately owned computer be sacrosanct?

That's what Rhonda Hall and Bonita Bourke thought. Three years ago, they were hired by a California subsidiary of Nissan to set up and run the electronic mail networkthat links the car company's Infiniti dealers. A female supervisor heard

that some of their E-mail was getting pretty steamy and began monitoring the messages. She soon discovered that the two had some disparaging things to say about her, and the women were threatened with dismissal. When Hall and Bourke filed a grievance complaining that their privacy had been violated, they were fired.

One might think the two employees had a strong case for unlawful termination. But their case was dismissed. Nissan's lawyers argued successfully that since the company owned the computer system, its supervisors had a perfect right to read anything created on it. "I'm dismayed," says Noel Shipman, the attorney who is handling Hall and Bourkes's appeal. "To me, the simple bottom line is that gentlemen don't read each other's mail."

But it's not that simple. The Electronic Communications Privacy Act of 1986 prohibits "outside" interception of E-mail by a third party--the government, the police or an individual--without proper authorization (such as a search warrant). It does not, however, cover "inside" interception-seeking a peek at the office gossip's E-mail, for example. In the past, courts have ruled that interoffice communications were considered private only if employees had a "reasonable expectation" of privacy when they sent it.

The fact is no absolute privacy exists in a computer system, even for the boss. System administrators need to have access to everything in a computer in order to maintain it. Moreover, every piece of E-mail leaves an electronic trail. Though Oliver North tried to delete all his electronic notes in order to conceal the Iran-contra deal, copies of his secret memos ended up in the backup tapes made every night by the White House system operators. "The phrase 'reasonable expectation of privacy' is a joke, because nobody reasonably expects any privacy nowadays," says Michael Godwin, general counsel for the Electronic Frontier Foundation, a not-for-profit group devoted to protecting the civil liberties of people using electronic networks.

Some computer users are taking matters into their own hands. If the law will not protect the privacy of their E-mail, they'll do it themselves--by scrambling their messages with encryption codes. Godwin's group is advocating that the government let private individuals use the most powerful encryption systems--systems that even the FBI can't crack. Unfortunately, such complex codes are likely to undermine the principal virtue of electronic mail: convenience. In the end, people bent on private communication--or government officials involved in criminal conspiracies--had best pick up the phone, or better yet, stroll down the hall and have a good old-fashioned face-to-face conversation.

**********END OF ARTICLE**********

++++++++++++++++++++++

```
+                      +
+    WHAT'S NEW?       +
+                      +
++++++++++++++++++++++++
```

The AIS Security Branch's Electronic BBS number has changed. Bureau telephone changes at the Parkersburg location have been completed and the 420 prefix has been replaced with a 480. The new BBS number is (304) 480-6083.

A new feature starts with this issue of the ISSM, titled "Jim's Corner". This article, written by Jim Heikkinen, will list Security Branch Training offerings; various computer security Videos; CBTs; and publications available to Bureau personnel through the AIS Security Branch.

**********END OF ARTICLE**********

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%                                    %
%    QUESTIONS ON SECURITY TOKENS    %
%          By Kim Reese              %
%                                    %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

In the last issue of the ISSM, an article was published describing security tokens and Public Debt's plans to implement this technology in 1994. As a result, several questions about the tokens were received. We felt that others may have had the same questions and decided to publish them with their responses.

1) What do the Tokens look like?
   The Tokens resemble a small pocket calculater.
2) How big are the Tokens?
   The Tokens are approximately 2 1/2" x 3 3/4" in its case. The actual Token itself is the size of two credit cards stacked together.
3) Will I have to have the Token with me at all times? I.E. carry it with my BPD I.D.
   No, you can secure your Token in your desk unless you are required to have dial-in access from home in order to perform your job function.
4) How many steps is this adding to my Logon?
   Approximately three steps plus Logon I.D. and mainframe password. The Security branch is looking at purchasing software that would allow you to log directly into the mainframe at the fifth step.
5) Do I take the Token home with me?
   No, unless you require dial-in access from home.
6) What happens if I loose the Token?
   If your Token is lost notify your ISSM. The ISSM will provide you with another Token and notify the other ISSMs and OAIS Security branch to be aware of the missing Token.
7) What happens if the Token breaks?

If your Token breaks notify your ISSM. The ISSM will replace your Token with a new one and return the faulty Token to the OAIS Security branch to be returned to the contractor for repair or replacement.

8) What if I forget my PIN number?
Contact your ISSM. If you have not changed your PIN number the ISSM is able to determine the PIN number of your Token through the OAIS Security branch. If you have changed your PIN number the ISSM will replace your Token and provide the PIN number assigned to the new Token.

9) If I loose my Token and someone else finds it can they use my Token?
No, The other person would need to know your PIN number in order to activate your Token.

10) Could someone borrow my Token to gain access if they cannot find their Token?
No, the other person would need access to both your PIN number and your Logon I.D./Password.

11) Do the Tokens need to be LOCKED UP when we are not using them?
Yes, the Tokens should be kept in a secured area. (i.e. locked in your desk)

12) Is the LOGON complicated using the Tokens?
No, you will be provided short, concise step-by-step instructions on the process and one-on-one training.

13) Who do I contact if the Token is not functioning properly?
You contact the Command Center, just as you do for other mainframe questions.

14) You mean I have to learn a new PIN number every time the battery goes dead on the Token?
Yes, the contractor will probably do all maintenance of the Tokens including changing batteries. We are not equipped or trained to properly maintain the Tokens, therefore this was included in the procurement contract.

15) Do the Tokens need to avoid severe temperature changes?
Yes, this should not be a problem if the Token is left in your desk.

16) What kind of training will be provided on the Token use?
Token training will be done on a one-on-one basis with each user by their ISSM until the user is comfortable with the Logon process.

17) When is the implementation date for the Tokens?
Implementation for the Tokens is tentatively scheduled for March 1994.

18) To whom do I report a missing Token.
Report missing Tokens to your ISSM who will notify OAIS Security branch of the missing Token.

19) Will we be financially responsible for a lost or broken Token?
No, the procurement contract covers maintenance issues.

Please forward any additional questions to the OAIS Security Branch or a member of the Token Committee. The committee members are Kim Clancy, Dana Whited, Mary Clark, Glenn Siber, Kim Reese and Sandra Woods.

**********END OF ARTICLE**********

```
XXXXXXXXXXXXXXXXXXXXXXXXXX
X                         X
X         CLYDE'S         X
X    Computer Security    X
X      Hall of Fame       X
X                         X
XXXXXXXXXXXXXXXXXXXXXXXXXX
```

Patrick Conner, ISSM for the Office of Administration, Division of Management Services has been inducted to the Computer Security Hall of Fame.

Patrick Conner's dedication to his ISSM responsibilities are impressive. Upon Pat's assignment as an ISSM, his commitment to ensuring the success of the Division of Management Services security program was evident. Pat accepted his new responsibilities with enthusiasm and was obviously concerned about "doing the job right." Pat has assisted in blazing new ground for the security program when he educated application development teams in his area of their responsibilities in regards to security. Pat contacted the AIS Security Branch and requested a meeting so that all members of the development team could be made aware of their security responsibilities during development of the project. This is an impressive accomplishment for both Pat and Public Debt. It ensures that applications are installed with security in mind and aids Public Debt in enhancing the integrity of its computing program. Pat's dedication to ensuring that the job is done right the first time is a valuable one. Thanks Pat for a job well done.

Submitted by Kim Clancy, Manager of the AIS Security Branch

**********END OF ARTICLE**********

```
{{{{{{{{{{{{{{{{{{{{{{{{{
{                         {
{    VIRUS ALERT          {
{                         {
{{{{{{{{{{{{{{{{{{{{{{{{{
```

The following information was received from the Office of Information Resources Management...

This is to advise you that the Mint has encountered virus problems with PCs rented by Price-Waterhouse Corporation for work being conducted at the bureau. The Mint ADP staff identified computer viruses in the equipment Price-Waterhouse brought to the Mint. To date, the Mint has found two viruses which have affected five of the Price-Waterhouse PCs and 60% of their disks. By taking immediate action, the Mint was able to eradicate the viruses, save the Price-Waterhouse data, and prevent the viruses from spreading to the Mint's own nationwide computer network.

Of particular concern to the Mint is the discovery that Price-Waterhouse apparently has known that it has had virus problems in its own offices for approximately 9 months. Since Price-Waterhouse may be working with bureaus other than the Mint, we are alerting you of this situation, and suggest that action be taken as appropriate within your bureau to ensure that your systems are not infected.

**********END OF ARTICLE**********

++++++++++++++++++++++++++
+ DEAR CLYDE +
+ +
++++++++++++++++++++++++++

Responses to questions for those who are searching for the truth.

Dear Clyde,

I have information on my PC I want to protect. Do you have any suggestions about PC security techniques?

R. Concerned

Dear Concerned,

The easiest way to secure data on your PC is to install programs which will require a password to gain access to your data. For most PCs, a boot-up password can be installed by running the set-up program for your PC. Also, files can be password protected within such applications as WordPerfect, Dbase and Lotus. If your PC does not have a password protection feature, there are programs such as PW62.ZIP, SECURE.EXE, ENCRYPT.EXE, DECRYPT.EXE, and PASSWORD.EXE available from the AIS Security Bulletin Board.

Another measure of security is to guard against destructive virus files being loaded onto your PC. There are virus detection programs available such as Central Point, Commcrypt, F-Prot, and Vader to aid you in detection of such virus codes.

Always remember when leaving your area, if you activate software which will require a password to be entered prior to your PC being able to be used, your data will be secured.

If you need help installing any of these programs, your ISSM can help you.

Send your comments or questions to Clyde c/o the AIS Security Branch in Parkersburg, Room 107F, or leave them in Clyde's mailbox located on the Security bulletin boards throughout the Parkersburg office.

**********END OF ARTICLE**********
==========

```
=                           =
=          TOKEN DEMO       =
=         by Mary Clark     =
=                           =
============================
```

A Security presentation was delivered by Kim Clancy, AIS Security Branch Manager, to the Executive Board (E-Board) introducing the Computer Security Issues and options facing Public Debt. As a result, it was determined that Public Debt's mainframe would be protected by the use of randomly generated passwords using a DES compliant token device. Such passwords change at each logon attempt and are therefore considerably more secure than the "static passwords" that we now use.

Beginning in March, 1994, all Bureau of Public Debt mainframe users will be required to use a token-generated password device.

A token implementation team was organized, and an implementation plan was developed that included the steps involved in the implementation of token controls on the mainframe. One of the tasks identified by the team to be completed before implementation was user awareness of the tokens.

As part of the awareness plan, a token demonstration was set up at E-Street (Room 527), C-Street (Room 223), and Parkersburg (In the front hall under Security branch's bulletin board, main building). This simple demonstration is an imitation of how the tokens will be utilized to improve the security of our mainframe computer system. It requires approximately five steps to gain access to the mainframe. These steps include:

1. Entering a user name.
2. Entering a fixed password.
3. Entering a PIN number to activate the token.
4. Entering a password from the PC into the token.
5. Entering the token generated password into the PC to gain access.

Although the logon procedure will vary slightly with the mainframe software, this demonstration gives a general idea of the steps involved with the token technology. Included with the demonstration is a handout listing questions and answers on Security Tokens. The handout answers the most frequently asked questions about the security tokens.

Any questions or comments regarding the demonstration should be directed to your ISSM or one of the token team members. The token team consists of: Kim Clancy, Mary Clark, Kim Reese, Glenn Siber, Dana Whited, and Sandy Woods.

**********END OF ARTICLE**********

```
!!!!!!!!!!!!!!!!!!!!!!!!!
!                         !
```

```
!      JIM'S CORNER       !
!    by Jim Heikkinen     !
!                         !
!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Starting with this issue I will offer training opportunities for anyone who desires a security "tune-up".

Initially, however, some background information is required to provide insight into the Security Branch security awareness training mission.

The AIS Security Branch is mandated by the Computer Security Act of 1987, Public Law 100-235, to provide "...mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each federal computer system within or under the supervision of..." the Bureau of Public Debt.

Further, the branch follows the guidelines and standards developed by the National Institute of Standards and Technology (NIST) in providing this required training. NIST Special Publication 500-172 may be considered the training "bible" in that all employee categories, subject matter areas and training levels are provided for in a matrix of training activities that satisfies the exigencies of P.L. 100-235. I'll expand each category and explain how each applies to our individual security responsibilities in future issues of the newsletter.

Also, samples of opportunities for refresher training and interesting audio-visual materials will be offered.

Formal training to be announced:

ACF2 - Washington (contract award is imminent)
SNA/APPN/APPC - IBM Network Architectures
Novell NetWare Security - Novell specific security issues

Publication: (Available on request basis through the Parkersburg AIS Security Branch.)

"Computer Addiction? A study of computer dependency" by Margaret A. Shotton

**********END OF ARTICLE**********

```
################################################
#                                              #
#              COMPUTER SPEAK                  #
#    COMPUTER TERMS AND THEIR MEANINGS         #
#                                              #
################################################
```

DES (Data Encryption Standard) ... an encryption method approved as a standard by the U.S. National Institute of Standards and Technology (NIST) and the American National Standards Institue (ANSI) for encoding nonclassified sensitive digital information.

eavesdrop ... Unauthorized interception of information. Usuallly refers to passive interception (receiving information), rather than active interception (changing information.

encryption ... the transformation of original text (called plaintext) into unintelligible text (called ciphertext). Sometimes called "enciphering."

**********END OF ARTICLE**********

The AIS Security Branch Runs an Electronic BBS. Give us a call at (304) 480-6083. An electronic version of the ISSM is posted on the board and can be downloaded. Articles in the electronic version may include more detail in that we are not limited by space constraints as we are in the paper copy.

**********END OF ARTICLE**********