An FBI-View of Computer Crime

By Mountain Bill

An FBI senior agent spoke recently about his agency's role in the investigation of computer crime. The agent gave his talk to a group of data processing majors, and even though it's possible that these students knew what a computer was, the fibbie assumed that his audience was harmless. His speech provided an insight into FBI activities in computer crime, and he described the different categories of computer thievery.

The FBI devotes one fourth of its energies to the area of white collar crime, which includes financial swindles, copyright infringements (bootleg records & video tapes), bribery (remember ABSCAM?) and computer crime. Within the area of computer crime, banks are a favorite target. Willy Sutton, the infamous bank robber of the thirties and forties, explained his preference for banks by saying, "That's where the money is." In 1981, $195 million was liberated from the banking system through fraud, while bank robbers were only able to withdraw $55 million. The average take in a computer caper is $600,000, and there have been a couple of really big hits, including Stanley Rifkin's $10 million prize from the Security Pacific Bank in Los Angeles. In desperation the banks have turned to the FBI.

When the FBI is called in to investigate computer fraud, it first tries to determine the complexity of the crime, which then gives them clues about who the crooks might be. The agency has classified computer crime in six categories, in order of increasing difficulty. The first two ways to screw a system are to either alter the data going into, or coming out of the computer, or to interfere with machine operations, like swapping disk packs or dropping power to the computer. These two methods account for 58% of known computer fraud, and can be done by any data-entry clerk or computer operator. The next two methods are more challenging, and involve hacking computer programs and modifying data stored in secondary memory (disks). These tricks can be done by any apllications programmer, and account for about 35% of known computer fraud. The last two hacks are the most elegant: penetration of operating systems and compromising telecommunications systems. These can only be accomplished by sophisticated systems programmers and analysts, and account for only 7% of known computer fraud.

The fibbie explained a few techniques which are popular among computer crooks. The first technique is wiretapping, either directly or inductively. By monitoring a data line with a printing terminal, you can watch transactions travel down the phone line. Then after you see a couple passwords sail by, you log into the computer and peruse the database at your leisure. Another technique is what the FBI calls "between the lines" entry into a timesharing system. Supposedly there is a way to sieze a computer port when a user is logging out, giving you access to the computer with that user's privileges (perhaps the FBI dude was confused, and instead had in mind the login simulator technique described in TAP issue #71). Once in the system, you could install "trap doors" in various programs to provide new system (mis) features. And there is the piggy-back technique in which a microprocessor-controlled device is spliced in the dataline. The device intercepts all traffic on the line, analyzes it, performs any necessary changes, and then sends the data on its way.

How long does it take for the FBI to catch the computer crook? Well, first of all the FBI isn't sure if the crime will even be detected. Unlike a robbery or break in, there is no physical evidence of the crime. Some security systems keep audit records, but even these "electronic" witnesses can be erased by the clever hack. A bank may not even notice the money is missing for several months, and then may be too embarrassed to report the crime. Also, the FBI is unprepared to investigate complex computer crimes, and must hire outside consultants to help them find the culprits.

In spite of the FBI's efforts, computer systems will remain vulnerable until banks and corporations cough up the hundreds of thousands of dollars needed to protect their systems. Congress is dragging its heels on passing a computer crime bill, which leaves the FBI powerless to prosecute those crimes that aren't covered by the old-fashiond "fraud by wire" statute. Computer hackers have been given a short reprieve before 1984 and Big Brother arrives, so wise hackers would do well to get their act organized. Then after you accumulate some not-so-hard earned cash, go into the consulting business and sell your services to those poor victimized banks, corporations, and the FBI.

• Abbie Hoffman said that during his fugitive days he hatched a plan to expose lax security at the Brown's Ferry (Ala.) nuclear power plant by posing for a photo essay inside the grounds, but he chickened out at the last minute. He reveals in his new book that he and his cohorts got past the plant's guardhouse, but felt the actual photographing would risk arrest.

TAP
MA BELL IS A CHEAP MOTHER
SEPTEMBER 1982 No. 77

LATE BREAKING RUMOR:

The FBI is reported to have put pen-registers on the phone lines of Washington D.C. area turists using the MIT-AI machine via the Arpanet. Although this report comes from an FBI agent in the Washington area, there is good reason to believe that pen-registers have been installed on phone lines in other parts of the country, too. Paranoid hackers should remember that pen-registers print a line feed every time the phone is taken off the hook, so you should minimize switchhook jiggling in order to conserve paper.

JUST ANOTHER BREAK IN THE WALL

by Oz. Y. Mandias

"Comfortably Numb" N-Ethylamphetamine and A-Methylfentanyl, mentioned in my last column, are now Schedule I (the former as of Jan/'82). Analogue enthusiasts are advised to move on to other variations. See "N-Ethylamphet. - Evaluation & Control Recommendations" by the DEA (availble by Freedom of Information request) for further information.

Also, chemists should always check for radio "beepers" in their chemical purchases especially in the packing material or boxes and hidden in solvent cans/drums.

Freebase: Methylene cholride is much easier to obtain, is non-flammable and works just as well as ether. (See Dr. Atomic's previous columns.) A simple home production method for freebase is as follows: Take a large (2 gram) vial, fill 3/4 full with water, add some coke and dissolbe by heating in a boiling water bath. Add some baking soda to the coke/water solution and return to the boiling water bath for another minute or so. Remove the vial from the boiling wather with tongs, and cool under cold running wather while shaking constantly to form the rock of freebase. The rock is filtered by placing it on a common paper napkin.

Remember, avoid all needle drugs. The only dope worth shooting is Alexander Haig.

"We Shall Overkill" If your state has restrictive handgun laws, you can often pick up your favorite roscoe without showing identification, and avoid the waiting period and other B.S. by attending your local gun show. Many dealers at these shows will sell you a piece for cash on the barrel, no questions asked. A good talking cash bearer can usually get (at least in California) the unregistered hardware of choice on the spot. A good throwaway is the Raven. Priced under $75, it is a .25 auto and the most popular Saturday Night Special (Second Amendment Special, if you will) on the market. It's no Colt Python, but kills just as effectively - almost as well as U.S. Foreign Policy.

The KTW is one brand of green teflon-coated "super bullet" that will pierce kevlar vests and engine blocks quite neatly. Moves are being made to ban these armour-piercing wonders, so stock up while you can. Anyone with a cool source should drop me a line.

The Ruger 10/20 is a 10-shot .22 semi-auto carbine and an excellent buy at about $100. Fit it with a scope and silencer and load with explosive or poisen-tipped bullets for sniping or other "tweps" (term w/ext. prej.). Or for close-up action and crowd work, take out the disconnector pin (see the diagram that comes with the rifle) for full auto, fit with a folding stock and 2 25-round Condor banana clip mags stuck together for 50 round capacity, (see your local gun shop or mail order ads for these accessories) and you've got a cheap, simple SMG that's quite effective for any "wet work" you may have in mind

"Hey you, don't tell me there's no hope atall
Together we stand, Divided we fall...."

This is resident false prophet, Oz, signing off once more

IBM TIME SHARING OPTION (TSO) - PART II

- Nick Haflinger

I hope that everyone has experimented with the commands we learned last time because this month we are going to talk about SUBMITting jobs and running programs in the foreground (ie. inside the TSO region). Foreground jobs are helpful because snoopy operators will see very little of what goes on during your TSO session.

Important note- anytime you want to stop what you are doing hit the ATTENTION key. If your computer does'nt have one try the BREAK key. This should get the message COMMAND INTERRUPTED and *** which means hit the enter key to return to normal.

Now let's refer to your notes. Did you find some datasets to play with? When you type in "LISTD datasetname" it should reply like this:

```
"datasetname"
--RECFM--LRECL-BLKSIZE-DSORG
  FB     80    6160    PO
--VOLUMES--
  XXXXXX
```

RECFM is recording format, FB is fixed block. LRECL is logical record length while BLKSIZE is block size. DSORG is the dataset organization, PO being partitioned organization or a "library" dataset that contains multiple members. Keep trying until you find some good PO datasets.

Now see what is in the dataset by keying "LISTD dataset M" to get a member list. You can select a single member for edit by keying "EDIT datasetname(member)". You may need to also specify dataset type - ASM, DATA, or CNTL. It is a nuisance but sometimes you must say NONUM for unnumbered datasets. Remember if you get in trouble, type in HELP. Some more notes on EDIT are 1) if you hit the enter key twice you go into INSERT mode, just don't key anything and hit the enter key to go back into EDIT mode 2) to end an EDIT session without saving any changes type END NOSAVE 3) if you try to SAVE or END you might be prompted for a password, just hit enter a few times and get back to where you can say END NOSAVE.

If you have been lucky enough to get into a system with SPF or ISPF the job of snooping and changing can be much easier. To find out if your system has this use the "LISTA ST" command. A sample output follows:

```
--DDNAME---DISP--
datasetname
  ddname    disp
SYS1.UADS
  SYSUADS  KEEP
ISP.TEST.ISPPLIB
  ISPPLIB
```

The important item here is DDNAME which is your clue to what your terminal can get away with. The ddname ISPPLIB indicates that your terminal is able to use SPF. Key in SPF and find out! If SYSUADS is present then you can use the OPERATOR command. Don't try it now. Use the HELP OPERATOR command first to find out how to use it. The OPER command is very powerful and can be used to set up new accounts, change passwords, change priorities, cancel users, etc.

What we are going to do now is find out what datasets the host system has online. This is done with a LISTCAT command and it is preferable to do this in "batch" rather than "foreground". If you found a PO library dataset earlier you can look at its member list for interesting material. Since all batch jobs must have a jobcard, find a library that has a name ending in CNTL or ASM. These usually contain JCL (JOB CONTROL LANGUAGE) statements for running programs. Normally the programmer has these set up to run with valid jobcards and such. If you have SPF then scanning the libraries will be easy, follow the menu and don't save anything. However most of you will only be able to use standard TSO so pay attention and have fun.

First find a valid member and write down the jobcard which will look like //XXXXXXXX JOB (9999,xxxx,xxx) depending on the system. The first 8 X's are the jobname and you may want to use his jobname to minimize the chances of arousing the sleeping operator. The stuff inside the parenthesis is the job accounting data so don't try to improve on it.

Now let's create a member for ourselves. I will assume that you are using standard TSO. Enter "EDIT dsname(member)". Hopefully the dsname is one that you found allocated to your logon. Remember that dsnames might have to have apostophes around them and pick a member name that is not being used. This is what your screen should look like.

```
"EDIT TEST(NICK) asm"    (you key this in)
DATA SET OR MEMBER NOT FOUND, ASSUMED TO BE NEW
INPUT
00010_      (start keying following code here)

//jobname  JOB (put the jobcard here)
//STEP01   EXEC PGM=IDCAMS
//STEPCAT  DD DSN=SYS1.VSMASTER,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  LISTCAT CATALOG(SYS1.VSMASTER)
/*
```

Your catalog name may be different, see previous comments on LISTD and LISTC commands.

Of course if you find a member that you can use just CHANGE it as needed and then SUBMIT the job and then END NOSAVE. Before doing this use the HELP command to learn about the preceding CHANGE and SUBMIT commands. Also you must use the OUTPUT command to see the printout of any job you run. Make sure that the job says in the jobcard, "MSGCLASS=U" and all dd cards say "SYSOUT=*" or the operator will get your printout.

Next time we will have a lesson in basic IBM utilities and what they can do for you. This is just kinda off-the-cuff, so write me and let me know what you need to know. I WANT SOME FEEDBACK. Send it c/o TAP. Maybe I can set something up on one of the computer networks.

DOCTOR ATOMIC'S UNDERGROUND DRUG NEWS

LIFE EXTENSION: Deanol. (Syn Deaner. Chemical name—dimethylaminoethanol (DMAE)). Active and water soluble in its bitartrate and hemisuccinate forms. Reported to be a safe, natural stimulant that elevates mood, increases intelligence, and increases lifespan. (See Secrets of Life Extension by John Mann, p. 40, And/Or Press 1980, available from Loompanics.) Deanol is available without prescription from chemical supply houses and is inexpensive. Life extension dosage is 100-150 mg per day; therapeutic dosage is 300-400 mg a day, and CNS activity is strong enough to require a warning to take it in the morning to avoid insomnia. In addition to promoting life extension, Deanol may also get you high. As a scientific courtesy, would someone who has taken a therapeutic dose let us know if it is any good?

UP: Fencamfamine. Chemical name N-ethyl-3-phenylnorboranamine hydrochloride. This is a stimulant and anti-depressant. It's available from chemical supply houses OTC since it is not a controlled substance. Fencamfamine produces an effect somewhere between cocaine and methamphetamine, but it is not as powerful as either; however, it is euphoric. In England it's a prescription drug called "Reactavan", and is sold in 10 mg pills. A larger dose, 30 to 100 mg, may be needed to produce euphoric stimulation. Sniffing fencamfamine is harsh on the nose like methamphetamine, so it's best taken orally. Some people take it dissolved in coffee. The price is affordable: $30 to $70 for 50 grams from chemical supply houses.

BOOK: The MERCK INDEX is a chemical reference book that will become as indispensible and as used as your dictionary. The "Merck" is more comprehensive in many ways than the Physician's Desk Reference (PDR) because it gives data for many household and food chemicals as well as for drugs. Available from the Merck Co., P.O. Box 2000, Rahway, NJ 07065. Price is about $25.00.

HIGH VOLTAGE: A high tech pot garden was busted in Novato, CA — the police claim that their attention was drawn to the warehouse mainly because of a suddenly high consumption of electricity needed for halide lights. (See High-Times, May '81, p. 20 for details.) Electric heating mantles also drain a lot of power and may, therefore, also draw the attention of the DEA. See the TAP Index "Free Electricity" for electric meter jumping instructions. Don't advertise your lab or indoor farm with a high electric bill.

MORE ON COMPUTER SECURITY

by Simon Jester

In issue #75 I talked about a new way to break into large computers that has the experts shitting in their pants. Well, I found out how to do it about a week after I mailed in that article, so here it is. This will work on almost all mainframe (maxi) systems, and most mini systems too, but it won't work on a micro. The scam lets one person on one terminal take control of another person operating on another terminal, so naturally it won't work on a micro.

The system you are using must have a function that lets you send messages from one terminal to another. This is sometimes called interterminal mail service. It must also have intelligent terminals hooked up, or at least the terminal that you take over must be intelligent. The scam takes advantage of two features in the intelligent terminal, first the ability to send data in "block mode". This is where you enter data into the terminal and it stays on screen, in the terminals memory, without being transmitted to the host computer. You can then edit it, and when you are ready to send it, press a "send" key. The entire block of data will then be transmitted. The second feature you take advantage of is called "soft keys". To control the editing of the block of data, there are special keys, which generate control characters when pressed. These are interpretted appropriately by the terminal. The terminal can't tell if the control characters come from the keyboard or from the computer. So, the rest is obvious. You log on, and send some guys terminal a message putting it into block mode. Then you send the appropriate commands to put $20 million into your account. These are stored in the block of data to be later transmitted, since you are in block mode and the terminal can't tell it's keyboard from the host computer. Then you send the transmit signal. The terminal transmits the order for the extra $20 mil, and the computer, being stupid as a post, does what it has been ordered to by the terminal.

This lets you take control of another users workspace, and you can manipulate his data sets, copy out protected information, or generally get access to things that you aren't supposed to be able to get into. Now some of you are going to say "thats obvious, why waste TAP space with it?" But the point is, this scam isn't obvious. I knew about all the things that you need to do it for a long time, but I never thought of this until I heard about it. And the beauty of it is, it's so simple that there are almost no ways to protect against it.

There are several suggested ways of protecting against this scam. One is to disable the intelligent terminals. If you do this, you lose all the features of the intelligent terminal, so this isn't very practical. Another suggestion was to disable the interterminal mail service. This is also kind of a stupid idea since you lose the entire mail service capability. There was one practical suggestion by the security experts. Put a software filter in the computer that doesn't allow control characters to be sent from one terminal to another. This will keep you from taking control of the other terminal at all. I have a suggestion to get around this. The set of ASCII characters range from 0 to 127. Most filters will take out the control characters in that range. But there is also a duplicate set of ASCII characters from 128 to 255, with 128 corresponding to 0 and 255 corresponding to 127. These characters are identical to the first set, but they are called the high order characters because they have their highest priority bit set. They will do the same thing as the first set, but you can't generate them from your keyboard, you have to write a program and use the CHR$ function or its equivilant to generate a character from the high order set. Another suggestion is to try to find a different mail utility, one that might not have the filter. There are usually several. One usually lets two users talk directly. Another lets you leave messages for another user, who will look at them later. When he logs in, it may print out his messages, or inform him that he has a few. When he reads them, he gets blown off. The advantage of this is that you don't have to be logged on when he gets blown off his terminal, everything is prerecorded.

A few more hints. There is usually a function to lock the keyboard on a terminal. you may want to use this to keep the guy from trying to interfere as his account is getting fucked over. There may even be an option to supress printing on his screen. If there is, you may be able to do the whole scam quickly, then return control to him by unlocking his keyboard, and he might not even notice that anything happenned for a while. Another hint towards this end is, if you are doing the whole scam while you are on-line, to write a program which will do the whole thing. Then you just start it up, and sit back. The whole thing should be done in less than a second. If you can keep anything from showing on his screen, or clear his screen afterwards, he may not know anything happenned. Of course, you may want to set up a batch job or use the delayed message so you can say you weren't even logged on when the breakin happenned.

There is a report from SRI (Stanford Reasearch Institute), which I have sent to Tom. I'm sure he will send you a copy, but it isn't too good. (Thanks for the report,Donn. -Simon) There is also info on this scam in one of the January issues of InfoWorld (it comes out weekly). I don't know which issue, and in either the January or February issue of Science magazine. If you can get either, please send it to me c/o TAP. Keep on Phreakin' and don't get caught! -Simon

More Confusion About AUTOVON

by

Fred Steinbeck

After following the controversy about AUTOVON throughout the history of TAP, I thought I'd try a couple of military friends of mine and see what I could see.

After a little bit of digging, I came up with a Navy guy, who I shall call Jeff, for sake of argument.

Jeff told me what little he knew about AUTOVON, and much of it came as a surprise. First, he does not have a touch-tone phone on his desk; it's a rotary dial type (not only that, but he says he has never seen a touch-tone AUTOVON phone!). Second, I asked about the FOPIP signals (Flash Override, etc.) and he came back with a very surprising answer: AUTOVON no longer uses the FO signal, and it has changed the names of a few others. The new signals are:

FLASH: This signal seems to take the place of Flash Override. The official definition of this signal states that it is only to be used when there is a situation which is "immediately detrimental to the security of the United States."

IMMEDIATE: Immediate calls are the next lowest priority - they are calls whose information must get through in two hours or less.

PRIORITY: These calls carry information which must be put through in six hours or less.

ROUTINE: These calls are the normal type of calls which are made by AUTOVON users. That is, they are just calls which don't have too much to do with national security, etc.

According to Jeff, when he wants to make a call to another place on his base, he simply dials the four digit number. If he wants to use the Bell outside lines (to call home, for example), he dials '9' first, and then the number.

Now, for AUTOVON calls, he dials '8' first, and then the 7 digit AUTOVON number. Note that this only allows him to make ROUTINE calls - no Flash or other kinds of calls.

Assuming he were to want to make a call with a priority above Routine, he dials '0' for operator and says, "Operator, Immediate priority call to so-and-such, please." Now remember, AUTOVON numbers are seven digits. He says the operator then dials (with touch-tone, not rotary) two digits, and then what he thinks are his seven digits. So, assuming the operator were to have to dial '8' to access AUTOVON, then next digit should be the extra one - the one which tells what priority the call is!

I don't know how much of this is applicable to all AUTOVON systems - Jeff has only had experience with his phone, and I don't know how much he really knows, and how much is speculation on his part.

If you have any comments or questions, send them to me, Fred Steinbeck, c/o TAP, or better yet, write an article!

OK, BUDDY, LETS SEE YOUR REGISTRATION

By Cheshire Catalyst

As the Bull System begins its reorganization, we Phone Phreaks also have to start getting our act together as well. One thing that has come about in the wake of the new de-regulation of The Phone Company is the FCC Registration program.

Under this program, the FCC registers equipment that will be connected to the telephone line. This is so that TPC will be aware of what equipment may be connected to its circuits in case the big bad customer owned equipment blows up, and causes damage to nice, sweet telephone network.

If you are like most of us here at TAP, our equipment is Genuine Bell (as the new ads say), but comes to us via the Manhattan Pothole Company. The Manhattan Pothole Company is the outfit that digs the potholes in the streets around New York. The Phone Company then drives its trucks over the potholes, and equipment then, "Falls off the truck," as we say in the trade. Accordingly, it may be inconvienient to give TPC a registration number from the bottom of one of their phones. Therefore, It's time to begin the TAP Registration Program. We will publish the registration numbers of non-Bell equipment as a service to our readers. Please turn over any device you see connected to a phone line, write down what it is, what it does, and the FCC registration number, and ringer equivilance number. We'll publish them in future issues of TAP. Here's the first batch:

ITT Slimline (Touch-Tone)
FCC Reg # AS293P-70038-TE-T   USOC # RJ11-C
Ringer Equivilance 1.0A

Tel-A-Tone Ringer (Auxiliary Ringer)
FCC Reg # AZ389g-62695-OT-N
Ringer Equivilance 0.4B

Stromberg 2500 Desk Phone (Touch Tone)
FCC Reg # AS293P-70088-TE-T
Ringer Equivilance 1.0A

Crest Two Line Electronic Phone Model # E2-2500T
This goodie handles two phone lines.
FCC Reg # BL-685L-69731-TX-N   USOC # RJ41-C

Northern Telecom Rendevous (Touch Tone)
FCC Reg # AB6982-68817-TE-T
Ringer Equivilance 0.7A

Inmates build helicopter

CARSON CITY, Nev. — A plumber, a welder and an electrician locked in a maximum-security prison almost managed to build a helicopter because the staff "didn't see the significance" of parts scattered around the prison shop, an official says.

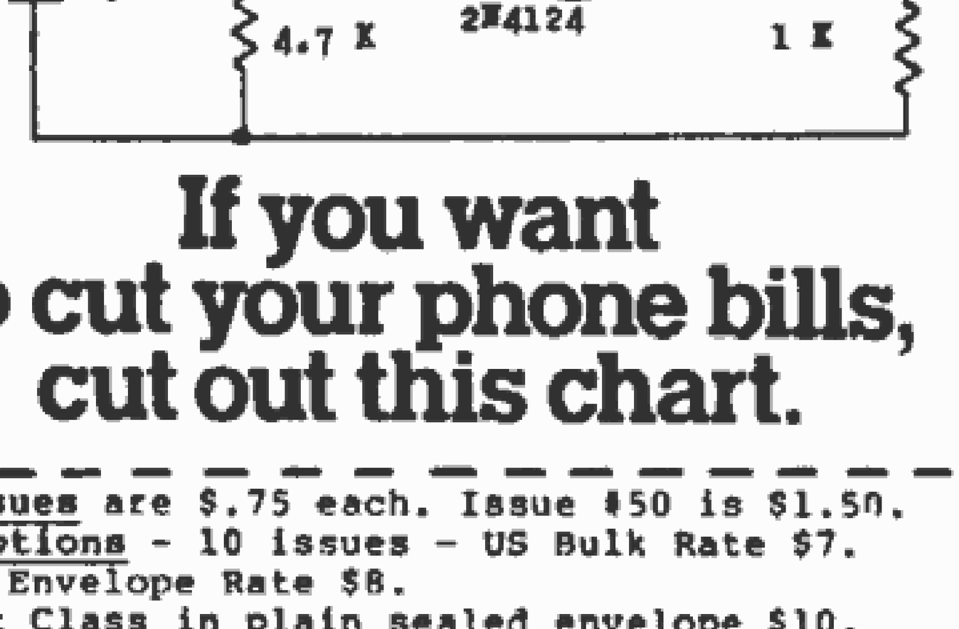
The inmates were short only the big rotor blade when their one-seat creation was found yesterday at the Nevada State Prison, officials said.

"We do have people in here who are journeymen, who are skilled craftsmen in their trades," said Vernon Housewright, the state prisons director.

Fussbuster

Tired of those half-assed cops always reporting you on their little radios? Well this ultra-simple circuit will jam all communications using FM such as FM radio, TV, 2 meters and of course cop radios. Its output ranges from about 50 to 900 MHz. The circuit needs from 9 to 16 volts and draws about 5 ma. The transistor can be any NPN general purpose such as the 2N3904 or 2N4124. The coil can be made by winding 9 turns of 18 or 20 AWG wire around a ½" DIA paper tube. This circuit can also be used as a mic by putting a carbon microphone (such as a telephone mouthpiece) in series with the battery.

The Stainless Steal Rat



TAP, Room 603, 147 W. 42 St., NY 10036

Bulk Rate
U.S. POSTAGE
PAID
Permit No. 3
Keansburg, N. J.

"'Tis time to get back to the *real* business of government . . . getting reelected"