The Information Systems Security Monitor

```
     _______     /--------\      /--------\     \         /|
        |        |               |               | \      / |
        |        |               |               |  \   /   |
        |         \_______        \_______       |    \     |
        |                 \               \      |          |
        |                 |                |     |          |
        |                 |                |     |          |
        |        \________/       \________/     |          |
      -------
```

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

===
Volume 2 Number 2   April 1992
===

///////////////////// In this Issue \\\\\\\\\\\\\\\\\\\\\\\\\

Hacker Lists Passwords Hackers Look For
Choosing the Right Password!

Imagine a hacker entering a system with your id and password because you did not take the time to choose a good password, this is something that can be completely prevented if people would take a few minutes to choose a good password. You must be creative when choosing a password not lazy. Since a password is usually the first line of defense against unauthorized access to a computer system, when the first line is broken the rest only take time. The average user usually has a password that is easy to select and easy

to remember. Any word that is easy to select or is contained in a dictionary is a poor and insecure selection for a password. The reason this makes a poor selection is because these words are the first ones an intruder will try when attempting to compromise your system. For instance, if your name is Tom Smith and your logon id is TSMITH your password should not contain any variation of these two words (Tom & Smith). A hacker will try TSMITH, SMITHT, TOMSMITH, SMITHTOM, TSMITH1, HTIMST, etc. before anything else.
As far as the length of a password goes its definitely the longer the better. To demonstrate this point I give you the following table:

# of Characters	Possible Combinations	Average Time To Discover	Example
1	36	6 min	q
2	1,300	4 hrs	bt
3	47,000	5 days	tyu
4	1,700,000	6 months	insw
5	60,000,000	19 years	potnb

etc...

The greater the number of possibilities a hacker must sort through, the better the chances of a password remaining undiscovered.

The best passwords are those that contain a combination of letters and numbers or are a combination of two or more unrelated words i.e. TREEFLOOR, TVBOOK, RADIOSHOE, etc. Another possibility is to select the initials of your two grandmothers combined with the number of times you have seen your favorite movie to come up with a password that resembles PAWH07, 07WHPA, PA07WH, etc.

If you think that you have chosen a password that is hard to guess or would take too much time to guess keep in mind that hackers have automated the process. There have been programs written for the sole purpose of guessing passwords, they take a list similar to the one in this article and try each and every one of them
These are the types of passwords that are hard to guess and will most likely not be found in any dictionary or word list. I am enclosing a list of common passwords that most hackers have a variation of, under no circumstances should you ever use a word contained in this list. All forms of profanity should also be included in this list. 100
666
6969
aaa
abc
abel

```
academia
academic
academie
access
ada
adele
adeline
adelphe
admin
adrian
aerobic
aerobics
agathe
agnes
aide
aime
aimee
airplane
alain
alban
albanie
albany
albatros
albatross
albert
alex
alexander
alexandre
alf
algebra
algebre
alias
aliases
alice
alida
alix
alpha
alphabet
alphonse
ama
amadeus
amandine
ambroise
amedee
ami
amorphe
amorphous
amour
```

amy
an
analog
analogue
ananas
anchor
ancre
andre
andromache
andy
angele
angerine
anicet
animals
animaux
anne
annie
annonciation
anselme
answer
anthelme
antoine
antoine-marie
anvils
anything
aout
apollinaire
apolline
apotre
aquin
arc
aria
ariane
aristide
armand
armel
arnaud
arrow
arsene
arthur
ascension
asd
asm
assise
assomption
athena
athenes
atmosphere

```
aubin
aude
audrey
augustin
automne
autoroute
avent
avila
avion
avril
aymar
aymard
aztecs
aztecs
azur
azure
bacchus
badass
bailey
balance
banana
bananas
banane
bande
bandit
banks
banque
baptiste
barbara
barber
barbier
bariton
baritone
barnabe
barnard
bart
barthelemy
bartman
basic
basile
bass
basse
basson
bassoon
batch
batman
baudouin
beach
```

```
beater
beaute
beauty
beaver
beethoven
belier
beloved
benedicte
benoit
benz
beowulf
berkeley
berlin
berline
berliner
bernadette
bernard
bernardin
bertille
bertrand
beryl
beta
everly
bicameral
bienheureux
bienvenue
bishop
bitch
blaise
bob
boris
bradley
brian
brice
brigitte
broadway
bruno
bsd
bumbling
burgess
cad
cafe
calude
camarade
campanile
cancer
cantor
capricorne
```

cardinal
careme
carine
carmel
carmen
carole
carolina
caroline
carson
cartouche
cascades
casimir
cassis
castle
castle
cat
catherine
cayuga
cecile
celine
celtics
cendres
cerulean
challenger
change
chantal
charles
charlotte
charmant
charming
charon
chat
chateau
chem
chemin
chemistry
chess
chester
cheval
chevalier
chien
chou
christ
christian
christine
christophe
cible
cigar

```
cigare
citroen
claire
clarisse
class
classic
classique
claude
clemence
clement
clotilde
cluster
clusters
code
coeur
coffee
coke
colette
collins
come
computer
comrade
comrades
conception
condo
condom
connect
console
constant
constantin
conversion
cookie
cooper
corinne
cornelius
couscous
create
creation
creosote
crepin
cretin
criminal
croix
cshrc
cyrille
daemon
dame
damien
```

```
dancer
daniel
danny
dapper
data
dave
davy
deb
debbie
deborah
december
decembre
default
defoe
defunts
delphine
deluge
denis
denise
desperate
develop
device
dial
diane
didier
diet
dieter
dieu
digital
dimanche
dimitri
disc
discovery
disk
disney
dog
dominique
donald
donatien
dos
drought
duncan
dupond
dupont
durand
dwladys
eager
earth
```

```
easier
easy
eatme
eau
edges
edinbourg
edinburgh
edith
edmond
edouard
edwige
edwin
egghead
eiderdown
einstein
elephant
elisabeth
elisee
elizabeth
ella
ellen
email
emeline
emerald
emeraude
emile
emilie
emma
enclumes
endeavour
enemy
engin
engine
engineer
entreprise
enzyme
epiphanie
erenity
eric
ersatz
establish
estate
estelle
ete
eternity
etienne
euclid
euclide
```

```
eudes
eugenie
evelyn
evrard
extension
eymard
fabrice
facile
fairway
famille
felicia
felicie
felicite
fender
ferdinand
fermat
fernand
ferrari
fete
fevrier
fiacre
fidele
fidelite
fidelity
field
file
filet
fini
finite
firmin
fishers
flakes
fleche
fleur
fleurs
float
flocon
flocons
florent
florentin
flower
flowers
foolproof
football
foresight
format
forsythe
fourier
```

```
fraise
framboise
francine
francois
francoise
fred
frederic
friend
frighten
fulbert
fun
function
fungible
gabin
gabriel
gaetan
games
gardner
garfield
gaston
gateau
gatien
gatt
gauss
gautier
gemeaux
genevieve
geoffroy
george
georges
gerard
geraud
germain
germaine
gertrude
ghislain
gibson
gilbert
gildas
gilles
ginger
gisele
glacier
gnu
golf
golfer
gontran
gorgeous
```

gorges
gosling
gouge
goutte
graham
grahm
gras
gregoire
group
gryphon
gucci
guenole
guess
guest
guillaume
guitar
guitare
gumption
guntis
guy
gwladys
habib
hack
hacker
hal
hamlet
handily
happening
harmonie
harmony
harold
harvey
hawaii
hebrides
heinlein
helene
hello
help
henri
herbert
hermann
hermes
herve
hiawatha
hibernia
hidden
hippolyte
hiver

```
homework
honey
honore
honorine
horse
horus
hubert
hugues
humbert
hutchins
hyacinthe
hydrogen
ibm
ida
ignace
igor
imbroglio
imbroglio
immaculee
imperial
include
inconnue
ines
info
ingres
ingress
ingrid
inna
innocent
innocuous
internet
invite
irene
irenee
irishman
irlande
isabelle
isidore
isis
jacqueline
jacques
janvier
japan
japon
jean
jean-baptiste
jean-claude
jean-francois
```

```
jean-michel
jean-pierre
jean-yves
jeanclaude
jeanfrancois
jeanmichel
jeanne
jeanpierre
jeanyves
jerome
jessica
jester
jeudi
jixian
joel
johnny
joseph
joshua
jour
judas
judicael
judith
juggle
juillet
juin
jules
julia
julien
julienne
juliette
jumeaux
jupiter
juste
justin
justine
kathleen
kermit
kernel
kevin
key
kirkland
kiwi
knight
ladle
lambda
lamination
landry
lapin
```

```
larissa
larkin
larry
laurent
lazare
lazarus
lea
lebesgue
lee
leger
leland
leon
leonce
leroy
lewis
library
licorne
light
lion
lisa
lisp
loch
lock
lockout
louis
louise
lourdes
love
luc
lucie
lucien
lumiere
lundi
lune
lydie
macintosh
mack
madeleine
madelene
maggot
magic
magique
mai
mail
maint
malcolm
malcom
manager
```

```
mangue
marc
marcel
marcelle
marcellin
mardi
marguerite
marie
marie-madeleine
marietta
mariette
marina
marius
mark
markus
mars
marthe
martial
martin
martine
martinien
marty
marvin
master
math
mathilde
matthias
matthieu
maurice
maxime
medard
melaine
mellon
memory
mercredi
mercure
mercury
meres
merlin
metro
mets
mgr
michael
michel
michelle
mike
minimum
minsky
```

```
mit
modem
modeste
mogul
moguls
monique
mont
moose
morley
morts
mouse
mozart
mutant
nadege
nagel
naissance
nancy
napoleon
narcisse
nasa
natacha
nathalie
nationale
nativite
navette
nepenthes
neptune
ness
nestor
net
network
new
news
newton
next
nicolas
nina
ninon
nobody
noel
norbert
notre
novembre
noxious
nuclear
nutrition
nyquist
oceanography
```

```
ocelot
october
octobre
odette
odile
odilon
office
olive
olivetti
olivia
olivier
open
operator
oracle
orca
orwell
osiris
outlaw
oxford
pacific
pacifique
pad
padoue
painless
pakistan
pam
paper
papers
papiers
paques
parfait
pascal
pass
password
pat
paterne
patrice
patricia
patrick
paul
paule
paulin
peche
pecheur
pecheurs
peggy
pelagie
pencil
```

penguin
penis
pentecote
peoria
percolate
peres
persimmon
persona
pete
peter
peugeot
peur
philip
philippe
phoenix
phone
pierre
pizza
plane
playboy
plover
pluto
pluton
plymouth
poire
poisson
poissons
polynomial
pomme
pondering
porc
pork
porsche
poster
power
praise
precious
prelude
presence
presto
prevision
prince
princeton
printemps
prisca
priv
private
privs

```
professor
profile
program
prosper
protect
protozoa
prudence
pub
public
pumpkin
puppet
quentin
qwerty
rabbit
rainbow
raindrop
raissa
raleigh
rameaux
random
raoul
rap
rascal
raymond
reagan
really
rebecca
regional
reine
remi
remote
renaud
renault
rene
reponse
requin
reseau
richard
rick
ripple
risc
rje
robert
robot
robotics
rochester
rodent
rodolphe
```

```
rodrigue
roger
roi
roland
rolande
rolex
romain
romano
romaric
romeo
romuald
ronald
root
rosalie
rose
rosebud
roseline
rosemary
roses
rosine
ruben
rules
ruth
sabine
sacre
sade
sagittaire
sainte
sal
sales
salome
samedi
samson
sandrine
saturn
saturne
saturnin
saxon
scamper
scheme
school
scorpion
scott
scotty
sebastien
secret
security
seigneur
```

```
sensor
septembre
serenity
serge
service
sesame
severin
sex
sharc
shark
sharks
sharon
sheffield
sheldon
shell
shiva
shivers
shuttle
sidoine
signature
silvere
simon
simple
simpsons
singer
single
smile
smiles
smooch
smother
snatch
snoopy
soap
socrate
socrates
solange
somebody
sophie
sossina
sourire
souris
souvenir
sparrows
spit
spring
springer
squires
stanislas
```

```
strangle
stratford
student
stuttgart
subway
succes
success
summer
sun
super
superuser
support
supported
surfer
suzanne
swearer
sylvain
sylvere
sylvestre
sylvie
symmetry
sys
sysadmin
system
tangerine
tanguy
tape
target
tarragon
tatiana
taureau
taylor
tech
telephone
temptation
tennis
tentation
terminal
terre
test
thailand
thailande
thecle
theodore
theophile
therese
thibault
thibaut
```

```
thierry
thomas
tiger
tigre
toggle
tomate
tomato
topography
tortoise
tortue
toussaint
toxic
toyota
trails
transfer
transfiguration
travail
trivial
trombone
tty
tuba
tubas
tuttle
ulrich
umesh
unhappy
unicorn
unix
unknown
uranus
urbain
urchin
util
utility
uucp
valentin
vasant
venceslas
vendredi
venus
ver
veronique
verseau
vertige
vertigo
vianney
vicky
victoire
```

```
victor
victorien
vierge
village
vincent
virgin
virginia
virginie
virus
visitation
visitor
viviane
vivien
volvo
wargames
warren
water
weenie
whatever
whatnot
whiting
whitney
wholesale
wilfried
will
william
willie
winston
wisconsin
wizard
wombat
woodwind
word
work
wormwood
wyoming
xavier
xaviere
xfer
xmodem
xyz
yaco
yang
yin
yosemite
yves
yvette
zap
```

zimmerman
zita
zmodem
zzz

Written by "The Butler", a hacker at heart, a Systems Administrator in real life who enjoys learning as much as possible about any given system including how to circumvent its security measures. He has written articles for various hacker magazines that deal with computer security. He currently administers a PC Network for a medium size business (250 people). He also lectures to various groups including Local EDP Auditors Association, User Groups, and Private Corporations on how to protect their systems from hackers like himself but who use their knowledge for mischievous purposes.

========================end of article=========================

Dear Clyde

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

Send your comments or questions to Clyde c/o the AIS Security Branch in Parkersburg, Room 1011, or leave them in Clyde's mailbox located on the Security bulletin boards throughout the Parkersburg office.

Dear Clyde,
What is the proper way to dispose of diskettes which are no longer able to be used? Are there security concerns here?
Peggy

Dear Peggy,
Yes there are security concerns as the data stored on the diskettes may still be readable, if someone wants to take the effort to retrieve it. Therefore the diskettes should be disposed of properly. Any method of destroying the diskette can be used. Cutting it up as you do a credit card that is no longer to be used is one method. However the important thing is to make certain the disk surface, that is the inner contents of the envelope or plastic case, is destroyed.

(Note: I personally prefer giving the disk several good whacks with my sword and lance to render it unusable.)

Clyde .... Sir Clyde?
Rumor has it that Clyde is to be recognized for his continuing efforts in the arena of computer security by being knighted. There will be more on this in the next issue, stay tuned.

=======================end of article=======================

```
..........................................................
             A Journey Behind (further behind)  .       .       .
  .
             .   .         .       .         .           ..
    .
              .   The Dark Side of CYBERSPACE  .     .       ..
.  .
                  .     .          .      .       .       .
  .
             Hackers in Their Illusive World:  .  A Response .
.    .

..........................................................
```

A Response by: Dispater
Editor in Chief of Phrack Inc. Magazine
InterNet: phracksub@stormking.com

First of all, I would like to thank Kim Clancy for providing me with the opportunity to reply to her article in the previous issue of the ISSM. I find myself agreeing with her on more issues than not. I read her piece on Cyberspace... Most of the article was good, but I felt unclear about what she was saying in the section titled "The Dark Side." So I have attempted to present a few things from this hacker's viewpoint and make a few points where I have disagreed with her. The ">" indicates Kim's previous writings.

>...What is scary to me in regard to some of the avenues is
>the ability for individuals to get to so many different
>types of information...

What scares me are the kinds of people who have access to the most personal parts of our lives compiled into data bases (like Information America) that are for sale to anyone who wants to pay the money or has the "power" to access it. Why does the government need to know my unlisted phone number? Is it really any insurance agency's right to know that I have a son or daughter that is about to turn age 16, and will soon need to buy auto insurance? I think I have the right not to be bothered by an onslaught of people that think they have something I want to purchase from them. If you really enjoy junk mail and computerized telephone sales calls you can thank these kinds of databases.

>I am not stating that I think information should be
>shielded from individuals.

The more diverse sources of information we can all access, the better off society will become. If we look at the past we can see how accuracy in books was improved drastically by the creation of the printing press. The scribes of kings and church figures were no longer relied upon as authorities of various subject matter. Information was made cheap and easily possessed by the common man. Therefore if someone disagreed with some book that was printed, he and his guild could write their version of what THEY found to be true. This promoted truth, accuracy, a deluge of human interaction, and free thought.

>...I once went to a presentation about hackers. The
>presenter told a story about a mother who took her child's
>computer modem out into the driveway and ran over it after
>her son had been arrested for hacking...

What was the parent doing while her child was hacking? Another thing we need to clarify is the use of the word "child." These are not often children. There is a certain level of mental development that must occur first. I don't know much about child psychology, but I'd say that most kids under the age of 13 would have a bit of difficult time understanding computer networking. Most people in the computer underground are at least 16. If they are not 16 years old almost every sysop I know, kicks them off the system. The young person should be allowed to explore in areas the parent might not agree with as long as he/she is willing to talk about it with the parent afterward. Why are required to water down and censor all information so that is safe and easily understandable to the "little children?" If there is a 12 year old that has network access and is reading USENET's ALT.SEX.BONDAGE, I think there is a greater problem involved than the type of information the nets carry!!

>While hackers spend time developing their skills and
>learning how to master cyberspace they also use cyberspace
>to share information about what they have learned.

This is the great benefit of getting involved. Everyone should own a computer because of this reason.

>Information has been found on how to steal long distance

>phone calls from the phone company, how to make a pipe bomb
>and how to perform satanic rituals before sitting down to
>hack.

It is not illegal to know how to do any of the previously mentioned things. As you mention later the information can also be found in such places like libraries. We need to keep a few things in perspective here. MOST of the information readily available on phone phreaking is so out dated, one couldn't hope to implement the use of such knowledge without most surely getting caught in an ESS(Electronic Switching System environment. Most of the United State's telephones are on such a system.

Secondly, most of the information available on explosives is very crude. Most of it isn't worth the time it took to download. Actually there is more information available in the library on that subject than in all the data bases in the world. I personally think this kind of thing is simply stupid. I will not print that kind of thing in Phrack. That kind of information is typed in from books, by people who don't have anything else to do.

In regards to "satanic rituals", it is difficult to make any comments about this because in all my years of calling BBS's and talking to other hackers, I have never seen such an animal. I have seen *THREE* articles on the Wiccan religion which is similar to white witchcraft, but it's not even close to anything satanic. However, other than this minuscule tidbit in cyberspace, the only things I've seen were things that were written as pranks and for joke purposes. It amazes me that if one person has written something or done something it is representative of the whole community. This is definitely not a responsible conclusion. If some people would just open their eyes to reality, they would not see a computer underground filled with "satanic, child molesting anarchists".

>I hesitate to write the above because I don't want people
>to avoid the technology. Everything I have found is in
>most libraries, but the accessibility of it through
>computers makes it much easier to obtain.

You hesitate with good reason and you are correct about all that information being already in your local library. The problem boils down to "digital censorship." Some people are saying it's OK for a library to have the aforementioned information, but it's NOT OK for it to be on my computer's hard drive.

In regards to that argument I say it is much easier to get the information from a library than the computer. Let's take a look at they facts. First of all, most libraries are FREE. On the other hand the average computer system (386/33) costs around $1500. Your typical 8th grader doesn't usually have that kind of cash.

The problem is that reality and virtual reality is the same for some of us. We will promptly ignore silly rules like "it's ok for some people to know certain things, but it's not ok for me to know the same bit of information."
In the information age we are all becoming much more aware of each other's presence. We are finding out that we are all very different. We each have some ideas that can easily shock others. These ideas can and are being challenged by the other people we interact with. Therefore, we should NEVER take the step back into the "electronic dark age."

The really funny thing about all this is, everyone in the United States IS a part of cyberspace, even though most of them don't want to recognize this fact. If your name is on a computer somewhere, you are in cyberspace! So you'd better become aware of your existence. Use it to learn and question why its there!
========================end of article========================

OAIS Employees Volunteer to Judge Student Contest

Every October, the Computer Learning Foundation, a non-profit educational foundation serving the United States and Canada, hosts Computer Learning Month. During that month, among other numerous activities, the foundation hosts numerous contests designed to encourage students, educators, and community members to explore new areas of using technology and to share their knowledge with others. These contests for students provide parents and teachers with an activity children can do today to begin thinking and learning about what it means to be a responsible user of technology. One of this year's contests was a student writing contest focusing on Adult Attitudes on the Value of Technology and Ethical Issues. Students were to interview one parent and one other adult, write a summary of their opinions on the value of technology in our lives and the ethical issues involved with using technology, then the students evaluated what they thought of the comments and opinions expressed by the adults they interviewed.

The Bureau of the Public Debt participated in this program with several OAIS employees, Gretchen Bergmann, Kim Clancy, Bill Dobson, Zephery Ellerson, Joe Kordella, Gary Smith, and Ed Alesius, volunteering their time to judge the students entries.

While the use of a computer was not required to create the critique many submissions showed an adept usage of various word processing, desktop publishing and graphics software.

This interchange between the professional environment and schools proved to be very enlightening. It is refreshing to see a group dedicate its effort to a much needed task, keeping schools up with technology and its responsible use.

========================end of article========================

QUICK FIX SECURITY

The following is a listing of some easy to do security controls that help a lot....

1. Set modem to answer after 4-5 rings.
2. Select a dial-up number from a different prefix or out of order from the rest of your office.
3. Use call back features.
4. Use proprietary software for your communications e.g., PC Anywhere IV.
5. Use special modems for encryption and access control e.g., Leemah Datacom.
6. Disconnect after a certain period of inactivity.
7. Do not allow certain userids' to have dial-up access.
8. Use caller id and call tracking.
9. Display a blank screen when a connection is made so the user has no clue what they have connected to.

========================end of article========================

COMPUTER SPEAK

COMPUTER TERMS AND THEIR MEANINGS

access n. The ability of a subject to view, change, or communicate with an object in a computer system. Typically, access involves a flow of information between the subject and the object (for example, a user reads a file, a program creates a directory).

cyberspace n. The world that is created by the connection of computers. Travels thru this environment can be vast and undefined just as space travel can be. This is the environment Cyberpunks call home.

database n. A collection of data items processible by one or more programs.

phreaking v. The art and science of cracking the phone network (so as, for example, to make free long-distance calls). By extension, security-cracking in any other context (especially, but not exclusively, on communications networks).

virtual reality n. 1. Computer simulations that use 3-D graphics and devices such as the Dataglove to allow the user to interact with the simulation. 2. A form of network interaction incorporating aspects of role-playing games, interactive theater, improvisational comedy, and "true confessions' magazines. In a virtual reality session, interaction between the participants is written like a shared novel.

Phrack Inc. Magazine n. An electronically published and distributed magazine that focuses on technical issues.

========================end of article========================

Comptroller General Decision on EDI

The Comptroller General of the United States has issued a decision that electronic data interchange (EDI) technologies, with enhancements such as message authentication and digital signatures, can create valid legal contractual obligations between the U.S. Government and the party with whom the agency contracts.

Digest

Contracts formed using Electronic Data Interchange technologies may constitute valid obligations of the government for purposes of 31 U.S.C. 1501, so long as the technology used provides the same degree of assurance and certainty as traditional "paper and ink" methods of contract formation.

Decision

By letter dated September 13, 1991, the Director, Computer Systems Laboratory, National Institute of Standards and Technology (NIST), asked whether federal agencies can use Electronic Data Interchange (EDI) technologies, such as message authentication codes and digital signatures, to create valid contractual obligations that can be recorded consistent with 31 U.S.C. 1501. For the reasons stated below, we conclude that agencies can create valid obligations using properly secured EDI systems.

Background

EDI is the electronic exchange of business information between parties, usually via a computer, using an agreed upon format. EDI is being used to transmit shipping notices, invoices, bid requests, bid quotes and other messages. Electronic contracting is the use of EDI technologies to create contractual obligations. EDI allows the parties to examine the contract, usually on video monitors, but sometimes on paper facsimiles, store it electronically (for example on magnetic tapes, on discs or in special memory chips), and recall it from storage to review it on video monitors, reproduce it on paper or even mail it via electronic means. Using EDI technologies, it is possible for an agency to contract in a fraction of the time that traditional practices take.

As NIST pointed out in its request, the "paperless" nature of the technology has raised the question of whether electronic contracts constitute obligations which may be recorded against the government. NIST is in the process of developing standards for electronic signatures to be used in various applications,*1 including the formation of contracts, but has been advised that section 1501 imposes a barrier to the use of electronic technologies by federal agencies in this regard.

Discussion

Section 1501 establishes the criteria for recording obligations against the government. The statute provides, in pertinent part, as follows:

> "(a) An amount shall be recorded as an obligation of the United States Government only when supported by documentary evidence of-
>
> > (1) a binding agreement between an agency and another person (including an agency) that is--
> >
> > > (A) in writing, in a way and form, and for a purpose authorized by law. . . ."

31 U.S.C. 1501(a) (1) (A).

Under this provision, two requirements must be satisfied: first, the agreement must bind both the agency and the party with whom the agency contracts; second, the agreement must be in writing.

Binding Agreement

The primary purpose of section 1501 (a) (1) is "to require that there be an offer and an acceptance imposing liability on both parties." 39 Comp. Gen. 829, 831 (1960) (emphasis in original). Hence the government may record an obligation under section 1501 only upon evidence that both parties to the contract willfully express the intent to be bound. As explained below, EDI technology provides both the agency and the contractor the means to electronically "sign" a contract.

A signature traditionally has provided such evidence. See generally 65 Comp. Gen. 806, 810 (1986). Because of its uniqueness, the handwritten signature is probably the most universally accepted evidence of an agreement to be bound by the terms of a contract. See 65 Comp. Gen. at 810. Courts, however, have demonstrated a willingness to accept other notations, not necessarily written by hand. See, e.g., Ohl & Co. v. Smith Iron Works, 288 U.S. 170, 176 (1932) (initials); Zacharie v. Franklin, 37 U.S. (12 Pet.) 151, 161-62 (1838) (a mark);Benedict v. Lebowitz, 346 F. 2d 120 (2nd Cir. 1965) (typed name); Tabas v. Emergency Fleet Corporation, 9 F.2d 648, 649 (E.D. Penn. 1926) (typed, printed or stamped signatures); Berryman v. Childs, 98 Neb. 450, 153 N.W. 486, 488 (1915) (a real estate brokerage used personalized listing contracts which had the names of its brokers printed on the bottom of the contract in the space where a handwritten signature usually appears).

As early as 1951, we recognized that a signature does not have to be handwritten and that "any symbol adopted as one's signature when affixed with his knowledge and consent is a binding and legal signature. B-104590, Sept. 12, 1951. Under this theory, we approved the use of various signature machines ranging from rubber stamps to electronic encryption devices. See 33 Comp. Gen. 297 (1954); B-216035, Sept. 20, 1984. For example, we held that a certifying officer may adopt and use an electronic symbol generated by an electronic encryption device to sign vouchers certifying payments. B-216035, supra. The electronic symbol proposed for use by certifying officers, we concluded, embodied all of the attributes of a valid, acceptable signature: it was unique to the certifying officer, capable of verification, and under his sole control such that one might presume from its use that the certifying officer, just as if he had written his name in his own hand, intended to be bound.

EDI technology offers other evidence of an intent to be bound with the same attributes as a handwritten signature. We conclude that EDI systems using message authentication codes which follow NIST's Computer Data Authentication Standard (Federal Information Processing Standard (FIPS) 113*2 or digital signatures following NIST's Digital Signature Standard, as currently proposed, can produce a form of evidence that is acceptable under section 1501.

Both the message authentication code and the digital signature are designed to ensure the authenticity of the data transmitted. They consist of a series of characters that are cryptographically linked to the message being transmitted and correspond to no other message. There are various ways in which a message authentication code or digital signature might be generated. For example, either could be generated when the sender inserts something known as a "smart card"*3 into a system and inputs the data he wants to transmit. Encoded on a circuit chip located on the smart card is the sender's private key. The sender's private key is a sequence of numbers or characters which identifies the sender, and is constant regardless of the transmission. The message authentication code and the digital signature are functions of the sender's private key and the data just loaded into the system. The two differ primarily in the cryptographic methodology used in their generation and verification.

After loading his data into the system, the sender notifies the system that he wants to "sign" his transmission. Systems using message authentication codes send a copy of the data to the chip on the smart card; the chip then generates the message authentication code by applying a mathematical procedure known a cryptographic algorithm. Systems using digital signatures will send a condensed version of the data to the smart card, which generates the digital signature by applying another algorithm, as identified in NIST's proposed standard. The card returns the just-generated message authentication code or digital signature to the system, which will transmit it and the data to the recipient.

Under either approach, when an offeror or a contracting officer notifies the system that he wants to "sign" a contract being transmitted, he is initiating the procedure for generating a message authentication code or digital signature with the intention of binding his company or agency, respectively, to the terms of the contract.*4 The code or the digital signature evidences that intention, as would a handwritten or other form of signature. Both, generated using the sender's private key, are unique to the sender; and, the sender controls access to and use of his "smart card," where his key is stored.

They are also verifiable. When the recipient receives the contract, either on his computer monitor or in paper facsimile, it will carry, depending on which approach is used, a notation which constitutes the message authentication code or the digital signature of the sender, necessary information to validate the code or the signature and, usually, the sender's name. The recipient can confirm the authenticity of the contract by entering the data that he just received and asking his system to verify the code or the digital signature. The system will then use the information provided by the sender and either verify or reject it.*5 Both approaches use a key to verify the message just received; however, the digital signature requires application of a different key from that used to verify a message authentication code. The change of any data included in the message as transmitted will result in an unpredictable change to the message authentication code or the digital signature. Therefore, when they are verified, the recipient is virtually certain to detect any alteration.

Writing

To constitute a valid obligation under section 1501(a)(1)(A), a contract must be supported by documentary evidence "in writing." As NIST pointed out, some have questioned whether EDI, because of the paperless nature of the technology, fulfills this requirement. We conclude that it does.

Prior to the enactment of section 1501, originally section 1311 of the Supplemental Appropriations Act of 1955, *6 there was no "clean cut definition of obligations." H.R. Rep. No. 2266, 83rd Cong., 2d Sess. 50 (1954). Some agencies had recorded questionable obligations, including obligations based on oral contracts, in order to avoid withdrawal and reversion of appropriated funds. See 51 Comp. Gen. 631, 633 (1972). Section 1501 was enacted not to restrict agencies to paper and ink in the formation of contracts, but because, as one court noted, "Congress was concerned that the executive might avoid spending restrictions by asserting oral contracts." United States v. American Renaissance Lines, 494 F.2d 1059, 1062 (D.C. Cir. 1974), cert, denied, 419 U.S. 1020 (1974). The purpose of section 1501 was to require that agencies submit evidence that affords a high degree of certainty and lessens the possibility of abuse. See H.R. Rep. No. 2266 at 50.

While "paper and ink" offers a substantial degree of integrity, it is not the only such evidence. Some courts, applying commercial law (and the Uniform Commercial Code in particular), have recognized audio tape recordings, for example, as sufficient to create contracts. See e.g., Ellis Canning Company v. Bernstein, 348 F. Supp. 1212 (D. Colo. 1972). The court, citing a Colorado statute, stated that the tape recording of the terms of a contract is acceptable because it is a "reduction to tangible form." *7 Id. at 1228. In a subsequent case, a federal Court of Appeals held that an audio tape recording of an agreement between the Gainesville City Commission and a real estate developer was sufficient to bind the Commission. Londono v. City of Gainesville, 768 F.2d 1223 (11th Cir. 1985). The court held that the tape recording constituted a "signed writing." Id. at 1228.

In our opinion, EDI technology, which allows the contract terms to be examined in human readable form, as on a monitor, stored on electronic media, recalled from storage and reviewed in human readable form, has an integrity that is greater than an audio tape recording and equal to that of a paper and ink contract. Just as with paper and ink, EDI technology provides a recitation of the precise terms of the contract and avoids the risk of error inherent in oral testimony which is based on human memory.*8 Indeed, courts, under an implied-in-fact contract theory, have enforced contracts on far less documentation than would be available for electronic contracts. See Clark v. United States, 95 U.S. 539 (1877). See also Narva Harris Construction Corp. v. United States, 574 F.2d 508 (Ct. Cl. 1978).

For the purpose of interpreting federal statutes, "writing" is defined to include "printing and typewriting and reproductions of visual symbols by photographing, multigraphing, mimeographing, manifolding, or otherwise." 1 U.S.C. 1 (emphasis added). Although the terms of contracts formed using EDI are stored in a different manner than those of paper and ink contracts, they ultimately take the form of visual symbols. We believe that it is sensible to interpret federal law in a manner to accommodate technological advancements unless the law by its own terms expressly precludes such an interpretation, or sound policy reasons exist to do otherwise. It is evident that EDI technology had not been conceived nor, probably, was even anticipated at the times section 1501 and the statutory definition of "writing" were enacted. Nevertheless, we conclude that, given the legislative history of section 1501 and the expansive definition of writing, section 1501 and 1 U.S.C. 1 encompass EDI technology.

Accordingly, agencies may create valid obligations using EDI systems which meet NIST standards for security and privacy.

Comptroller General
of the United States
Sept. 13, 1990

General Counsel
U.S. General Accounting Office
441 G. Street, N.W.
Washington, D.C. 20548

Dear Sir:

As you know, National Institute of Standards and Technology (NIST) has cooperated with the Department of Treasury and the General Accounting Office to develop an electronic certification system wherein a cryptographic Message Authentication Code (MAC) is used in place of a written signature to bind a certifying officer to a payment order. Several other agencies have expressed their interest in using this or a similar system as a substitute for a written signature. In fulfillment of our responsibilities under the Computer Security Act of 1987, NIST is now in the process of developing a public key based Digital Signature Standard (DSS) which is specifically designed for electronic signature applications and will provide at least the same degree of security as the MAC approach. We have attached the DSS Federal Register Announcement and draft DSS which is now issued for public comment.

We have often been told that legal impairments exist which prevent agencies from implementing electronic signatures to bind the federal government. The specific statute cited is 31 U.S.C. 1501. Before formally recommending these standards for contracting and financial management applications, I would like to request a General Accounting Office decision as to whether NIST standards such as Federal Information Processing Standard (FIPS) 113 and a finalized DSS may be used throughout the federal government to record obligations under 31 U.S.C. 1501. If you need any further information in order to make your decision please feel free to contact Miles Smid, (301) 975-2938, of my staff.

Sincerely,

James H. Burrows
Director, Computer Systems Laboratory

Enclosures

*1 The Congress has mandated that NIST (formally the National Bureau of Standards) establish minimum acceptable practices for the security and privacy of sensitive information in federal computer systems. Computer Security Act of 1987, Pub. L. No. 100-235, section 2, 101 Stat. 1724 (1988).

*2 FIPS 113 adopts American National Standards Institute (ANSI) standard X9.9 for message authentication. It outlines the criteria for the cryptographic authentication of electronically transmitted data and for the detection of inadvertent and/or intentional modifications of the data. By adopting the ANSI standard, FIPS 113 encourages private sector applications of cryptographic authentication; the same standard is being adopted by many financial institutions for authenticating financial transactions.

*3 A smart card is the size of a credit card. It contains one or more integrated circuit chips which function as a computer.

*4 NIST officials advise us that technology using message authentication codes and digital signatures will be available to both contractors and contracting officers for use in government contracting.

*5 For the sake of simplicity, this example does not describe the complicated system of controls used to ensure that (1) no human knows the sender's private key and (2) the information received from the sender for validating the message authentication code or digital signature is correct and accurate.

*6 Pub. L. No. 663, 68 Stat. 800, 830 (1954).

*7 Other courts, interpreting the laws of other states, have held that a tape recording is not acceptable. See Sonders v. Roosevelt, 102 A.D.2d 701, 476 N.Y.S.2d 331 (1984); Roos v. Aloi, 127 Misc.2d 864, 487 N.Y.S.2d 637 (N.Y. Sup. Ct. 1985).

*8 Of course, just as with any contract or other official document, an agency must take appropriate steps to ensure the security of the document, for example, to prevent fraudulent modification of the terms. Agencies should refer to NIST standards in this regard. See, e.g., FIPS 113 (regarding message authentication codes). In addition, agencies should refer to the GSA regulations regarding the maintenance of electronic records, see 41 C.F.R. 201-45.2, and to the Federal Rules of Evidence with regard to managing electronic records to ensure admissibility, see generally Department of Justice Report, "Admissibility of Electronically Filed Federal Records as Evidence," Systems Policy Staff, Justice Management Division (October 1990).

========================end of article========================

Security Hall of Fame Established

Clyde's Computer Security Hall of Fame is being established to recognize those who contribute above and beyond the normal call of duty in their performance of contributing to the advancement and enhancement of Public Debt's computer security program.

The first inductee to this much sought honor is Bob Settles. Bob came to Public Debt immediately upon his graduation from college in 1964. Apart from a two year stint in Vietnam, his first 18 years were spent with the Internal Audit Staff. Then, in 1982, he was selected to manage the AIS Security Branch and has served in that capacity ever since. During his tenure as manager, the Branch's responsibilities have grown steadily to keep pace with the emphasis placed on information systems security throughout the Government. Public Debt's security program is now among the most highly regarded in the Treasury Department.

Bob has recently accepted a Computer Specialist position with the Treasury Department at its main office in Washington, D.C.

Bob epitomized the best in seasoned management and his departure will be keenly felt. We wish him the best in his new position!

========================end of article========================

What's New?

ISSM's gain recognition in international publication

The Public Debt Computer Security Program and the ISSM's received international recognition when an article written by Kim Clancy and Joe Kordella was published in ISPNews in the Jan/Feb 1992 edition. The article presented the role computer security plays in the protection of critical information assets of Public Debt in an environment of rapid technological change. It stressed that the ISSM's are key players in the implementation of the security program.

New Security Branch Manager Selected

The selection of Kim Clancy as the Security Branch Manager completes the consolidation of the Branch in Parkersburg. Kim was previously a security analyst in the AIS Security Branch. Prior to that, she was a computer security analyst for the State of Arizona, for over three years. She was also a computer systems security officer in the United States Air Force.

========================end of article========================

The AIS Security Branch runs an Electronic BBS. Give us a call at (304) 420-6083. 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.

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) 420-6368

Editors: Kim Clancy
             Joe Kordella
             Ed Alesius
             Mary Clark

Downloaded From P-80 International Information Systems 304-744-2253