0001 MRI 01077/189

OO AFO FBIIP ALO

DE RUCNFB #0063 1891922

ZNY EEEEE

O 081834Z JUL 99

FM DIRECTOR FBI (288-HQ-1234199)

TO ALL FBI FIELD OFFICES/IMMEDIATE/

[redacted]

b7E

288-C-76

FBI - Indianapolis

Date Received: JUL 08 1999

(name)

(name)

(name)

(name)

(name)

(name)

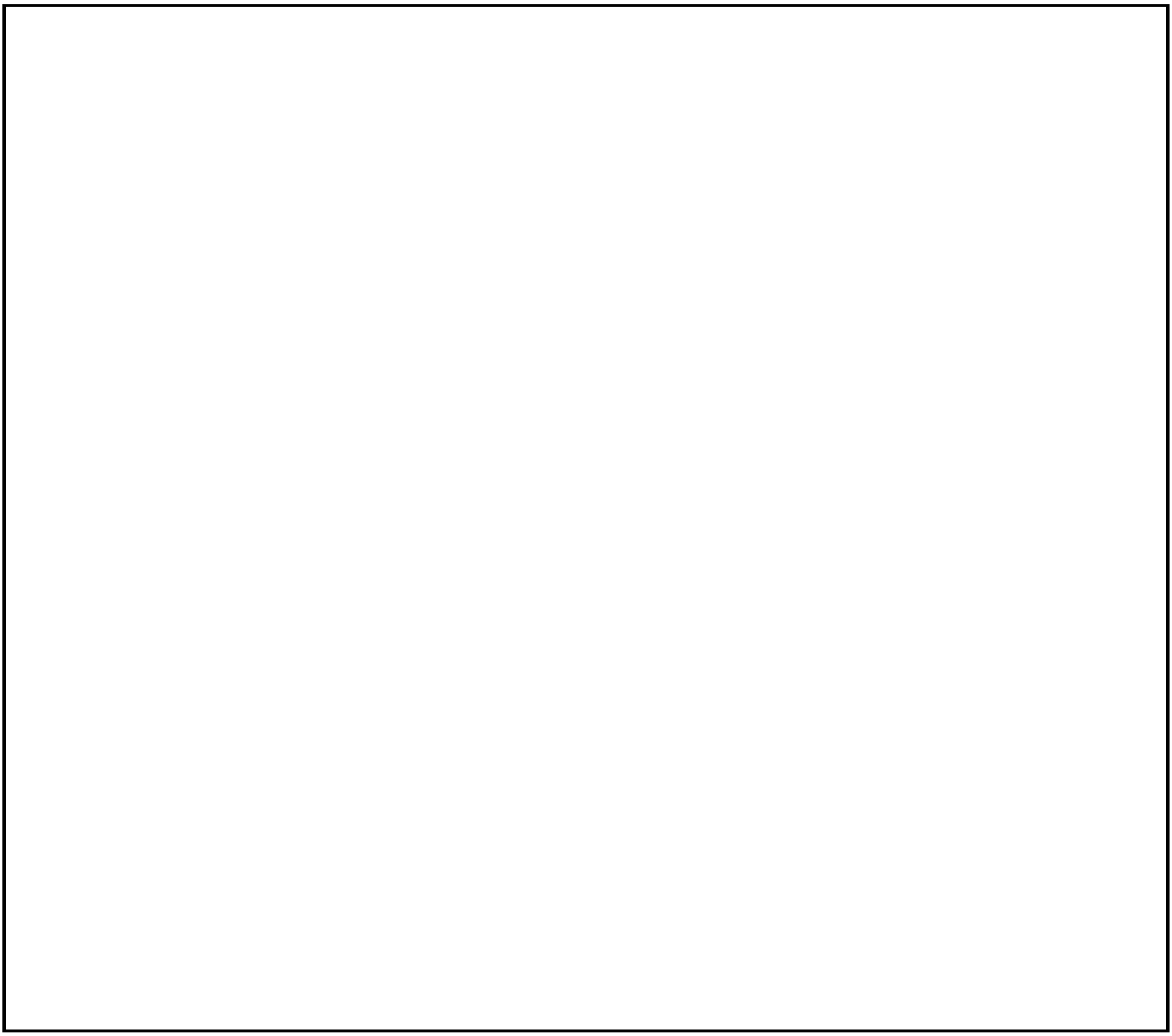
CO-5

Informational EC, only

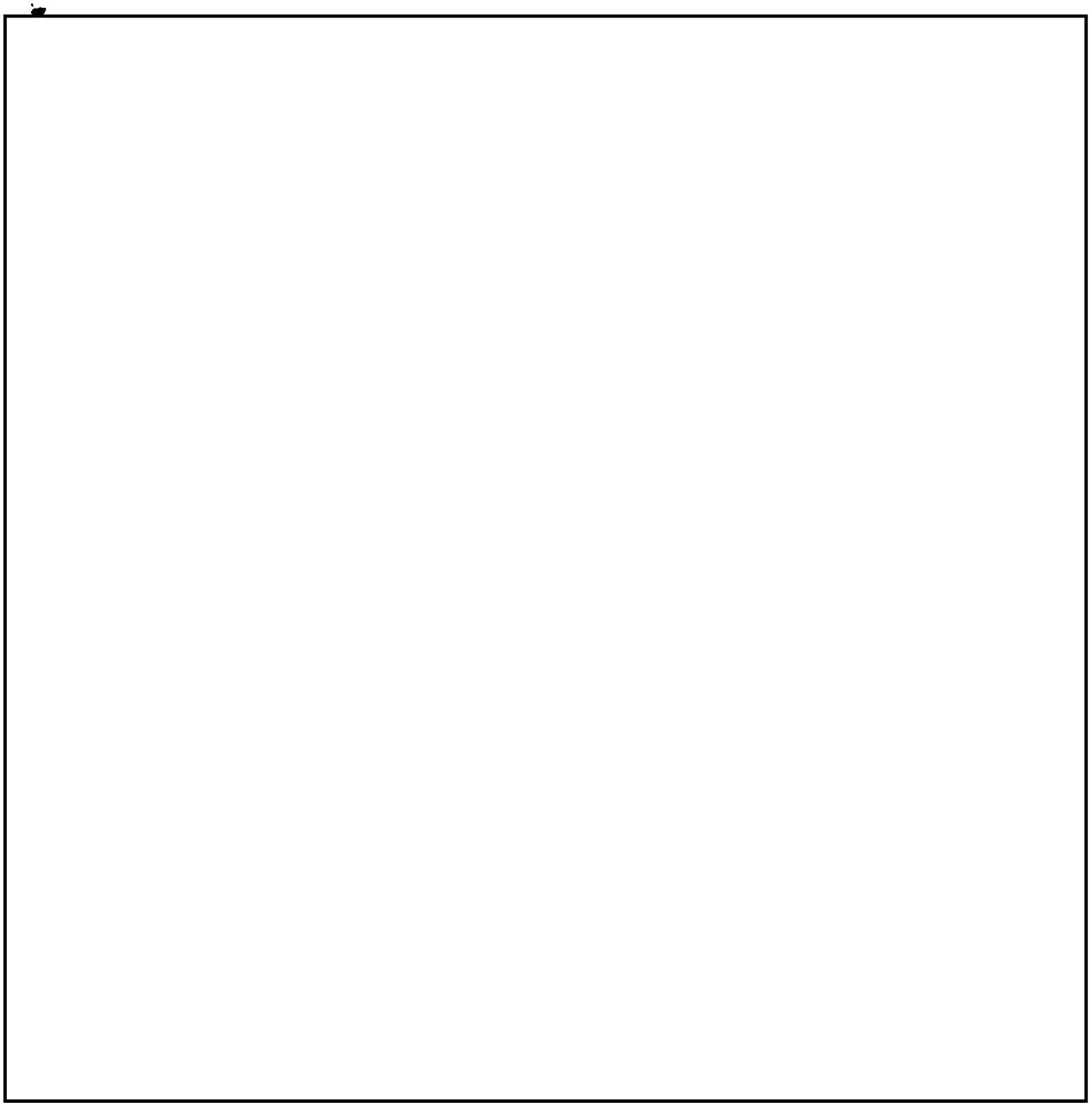
15cv999-226

[redacted]

b7E



b7E



b7E

BT

UNCLAS E F T O FOR OFFICIAL USE ONLY

SECTION ONE OF THREE SECTIONS

CITE: //1301//

PASS: NIC WARNING STAFF TO NATIONAL WARNING COMMUNITY; JTF-CND APPROPRIATE DOD FACILITIES, SERVICE COMPONENTS AND TARGET LOCATIONS; NIPC TO FEDCIRC, CARNEGIE MELLON CERT.

SUBJECT: NIPC INFORMATION SYSTEM ADVISORY (NIPC ADVISORY 99-016).

GROUP IN EXISTENCE SINCE 1984) RELEASED A PRODUCT CALLED QUOTE BACK ORIFICE UNQUOTE AT LAST YEAR'S DEFCON VI HACKER CONVENTION. CDC HAS ANNOUNCED PLANS TO RELEASE A NEW VERSION OF BACK ORIFICE (BACK ORIFICE 2000) ON JULY 10TH AT THE DEFCON VII CONVENTION LAS VEGAS. THE PRODUCT WILL BE MADE AVAILABLE AS A FREE DOWNLOAD ON THAT DATE.

2. (U) THE ORIGINAL 1998 RELEASE OF BACK ORIFICE INCLUDED THE FOLLOWING CAPABILITIES:

A. RETRIEVAL OF SYSTEM INFORMATION INCLUDING CURRENT USER, CPU TYPE, WINDOWS VERSION, MEMORY USAGE, MOUNTED DISKS AND DRIVE INFORMATION, SCREENSAVER PASSWORD, AND PASSWORDS CACHED BY USERS (DIAL-UPS, WEB AND NETWORK ACCESS, ETC).

B. FILE SYSTEM CONTROL: COPY, RENAME, DELETE, VIEW, SEARCH,

COMPRESS, AND DECOMPRESS FILES.

C. PROCESS CONTROL: LIST, SPAWN, KILL.

D. REGISTRY CONTROL: LIST, CREATE, DELETE, SET KEYS AND VALUES.

E. NETWORK CONTROL.

F. MULTIMEDIA CONTROL (INCLUDING SCREEN CAPTURE).

G. PACKET REDIRECTION AND SNIFFING.

H. APPLICATION REDIRECTION (SPAWN MOST APPLICATIONS ON A SPECIFIC PORT, SUCH AS TELNET).

I. HTTP SERVER (UPLOAD AND DOWNLOAD FILES).

J. RUNS ON START-UP WITH NO ENTRY IN THE TASK LIST.

3. (U) BACK ORIFICE 2000 WILL REPORTEDLY INCLUDE SEVERAL FEATURES NOT FOUND IN THE ORIGINAL VERSION, INCLUDING WINDOWS NT COMPATIBILITY (THE ORIGINAL PROGRAM ONLY WORKED ON WINDOWS 95/98), OPEN PLUG-IN ARCHITECTURE FOR 3RD PARTY ADD-ONS, STRONG CRYPTOGRAPHY, AND OPEN SOURCE CODE AVAILABLE UNDER GNU PUBLIC LICENSE.

4. (U) ASSESSMENT.

A. (FOUO) BACK ORIFICE 2000 WINDOWS NT COMPATIBILITY COULD

BT

#0063

NNNN

0002 MRI 01078/189

OO AFO FBIIP ALO

DE RUCNFB #0064 1891923

ZNY EEEEE

O 081834Z JUL 99

FM DIRECTOR FBI (288-HQ-1234199)

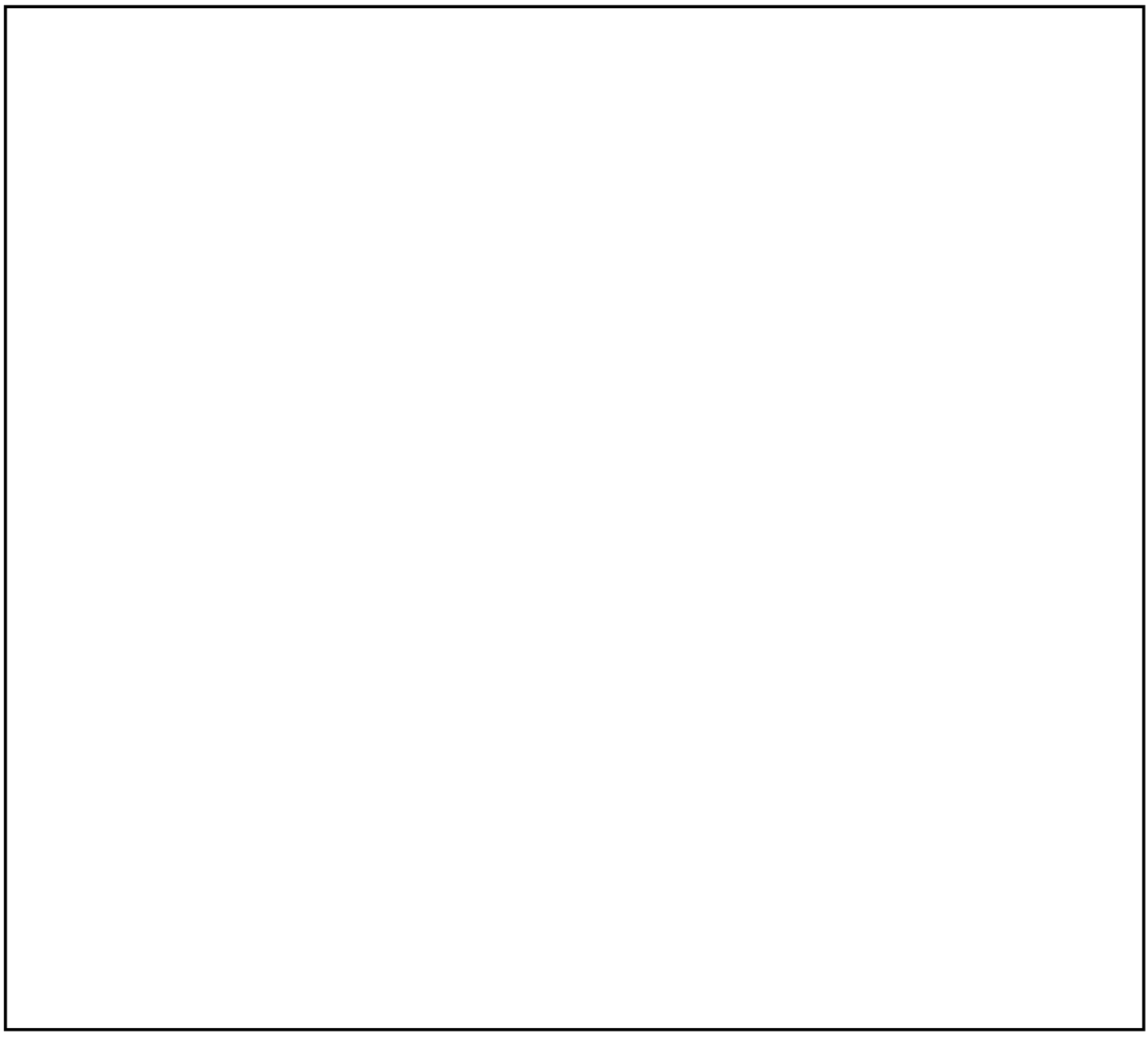
TO ALL FBI FIELD OFFICES/IMMEDIATE/

[redacted]

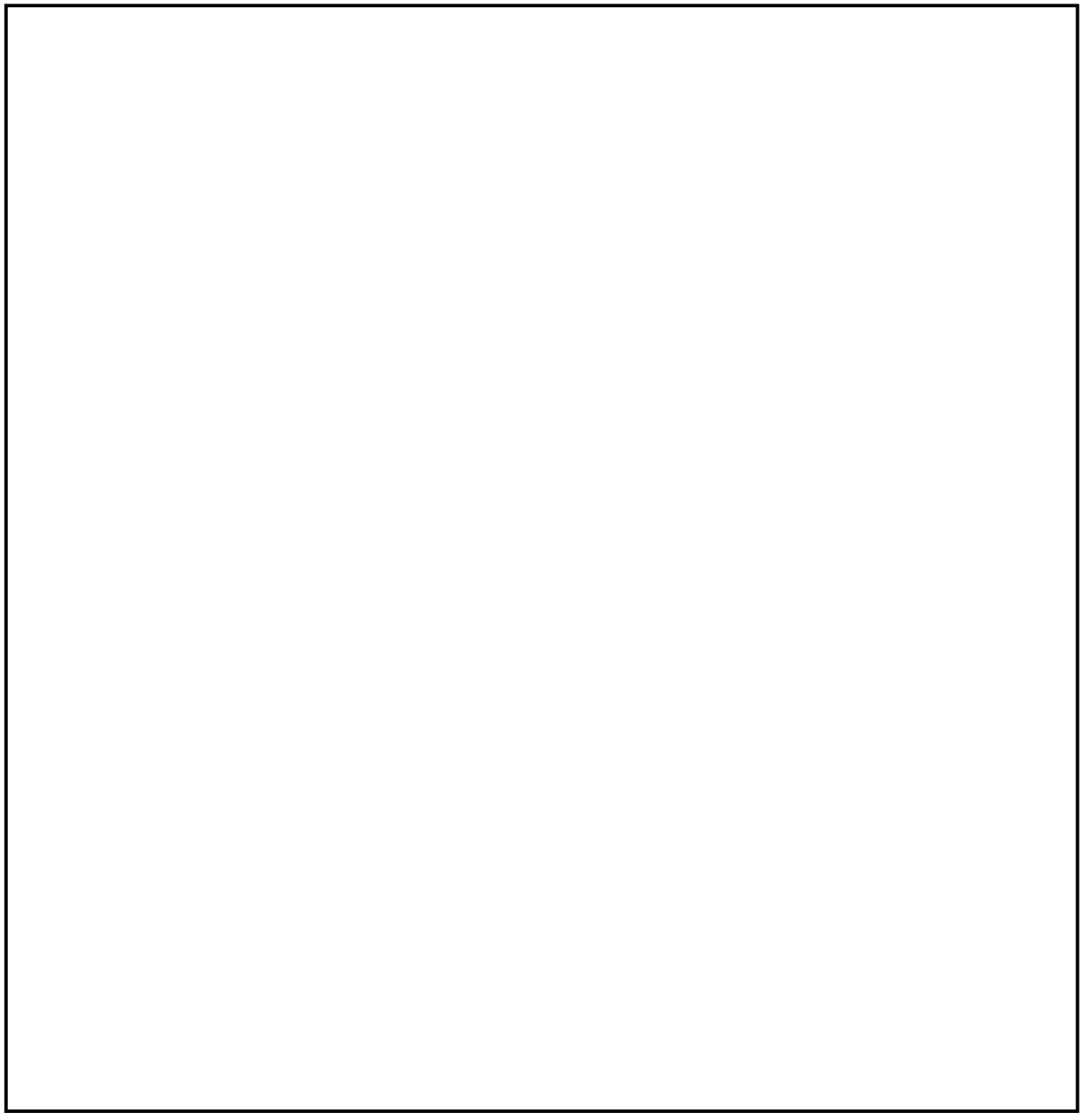
b7E

[redacted]

b7E



b7E



b7E

BT

UNCLAS E F T O FOR OFFICIAL USE ONLY

SECTION TWO OF THREE SECTIONS

CITE: //1301//

PASS: NIC WARNING STAFF TO NATIONAL WARNING COMMUNITY; JTF-CND APPROPRIATE DOD FACILITIES, SERVICE COMPONENTS AND TARGET LOCATIONS; NIPC TO FEDCIRC, CARNEGIE MELLON CERT.

SUBJECT: NIPC INFORMATION SYSTEM ADVISORY (NIPC ADVISORY 99-016).

TEXT CONTINUES:

GREATLY INCREASE THE POTENTIAL FOR DAMAGE TO NETWORK INFRASTRUCTURE. THE PREVIOUS VERSION ONLY AFFECTED WINDOWS 95/98 MACHINES, GENERALLY USED AS NETWORK CLIENTS. HOWEVER, INFECTION OF NETWORK SERVERS (COMMONLY RUNNING WINDOWS NT) COULD DRAMATICALLY INCREASE THE POTENTIAL IMPACT OF AN INFECTION IN TERMS OF BOTH DATA LOSS AND CONNECTIVITY DISRUPTION.

B. (FOUO) THE EXPECTED COMBINATION OF OPEN SOURCE CODE AND PLUG-IN ARCHITECTURE WOULD MAKE BACK ORIFICE 2000 POTENTIALLY MORE DESTRUCTIVE AND DIFFICULT TO ERADICATE THAN ITS PREDECESSOR. THE ORIGINAL BACK ORIFICE WAS FOLLOWED BY A SMALL NUMBER OF THIRD-PARTY ADD-ONS; IT APPEARS THAT CDC IS MAKING AN EFFORT TO ENCOURAGE THIRD-PARTIES TO ENHANCE BACK ORIFICE 2000, IN LINE

WITH THE GENERAL PHILOSOPHY OF OPEN-SOURCE PROGRAMMING ADVOCATES. EXPECT SIGNIFICANT VARIANTS TO APPEAR AFTER THE INITIAL RELEASE WHICH COULD INCLUDE VARIOUS PROPAGATION FEATURES, REMOTE INFORMATION TRANSMISSION, OR CORRUPTION AND DESTRUCTION OF DATA. THESE VARIANTS MAY REQUIRE ANTI-VIRUS SOFTWARE AND NETWORK PROTECTION UPDATES. EXPECTED BACK ORIFICE 2000 FEATURES COULD EASILY INCORPORATE CUSTOMIZED MALICIOUS CODE WITH THE BASIC PRODUCT.

5. (FOUO) RECOMMENDATIONS. BACK ORIFICE 2000 WILL LIKELY BE USED IN A SELECTIVE OR TARGETED MANNER SIMILAR TO PREVIOUS NETWORK SECURITY EXPLOITS. EXPECTED NT COMPATIBILITY WILL MAKE CORPORATE, GOVERNMENT, AND MILITARY SYSTEMS INCREASINGLY ATTRACTIVE TARGETS. THESE COMMONLY TARGETED GROUPS SHOULD AGGRESSIVELY REVIEW AND MONITOR COMPREHENSIVE SECURITY MEASURES TO PROTECT AGAINST THE KIND OF EXPLOITS CAUSED OR SUPPORTED BY BACK ORIFICE 2000. ADDITIONALLY, SUBSEQUENT MODIFICATION OF BACK ORIFICE 2000 FOR EXPANDED MALICIOUS IMPACT IS POSSIBLE, AND SHOULD BE IMMEDIATELY REPORTED.

BT

#0064

NNNN

0003 MRI 01079/189

OO AFO FBIIP ALO

DE RUCNFB #0065 1891925

ZNY EEEEE

O 081834Z JUL 99

FM DIRECTOR FBI (288-HQ-1234199)

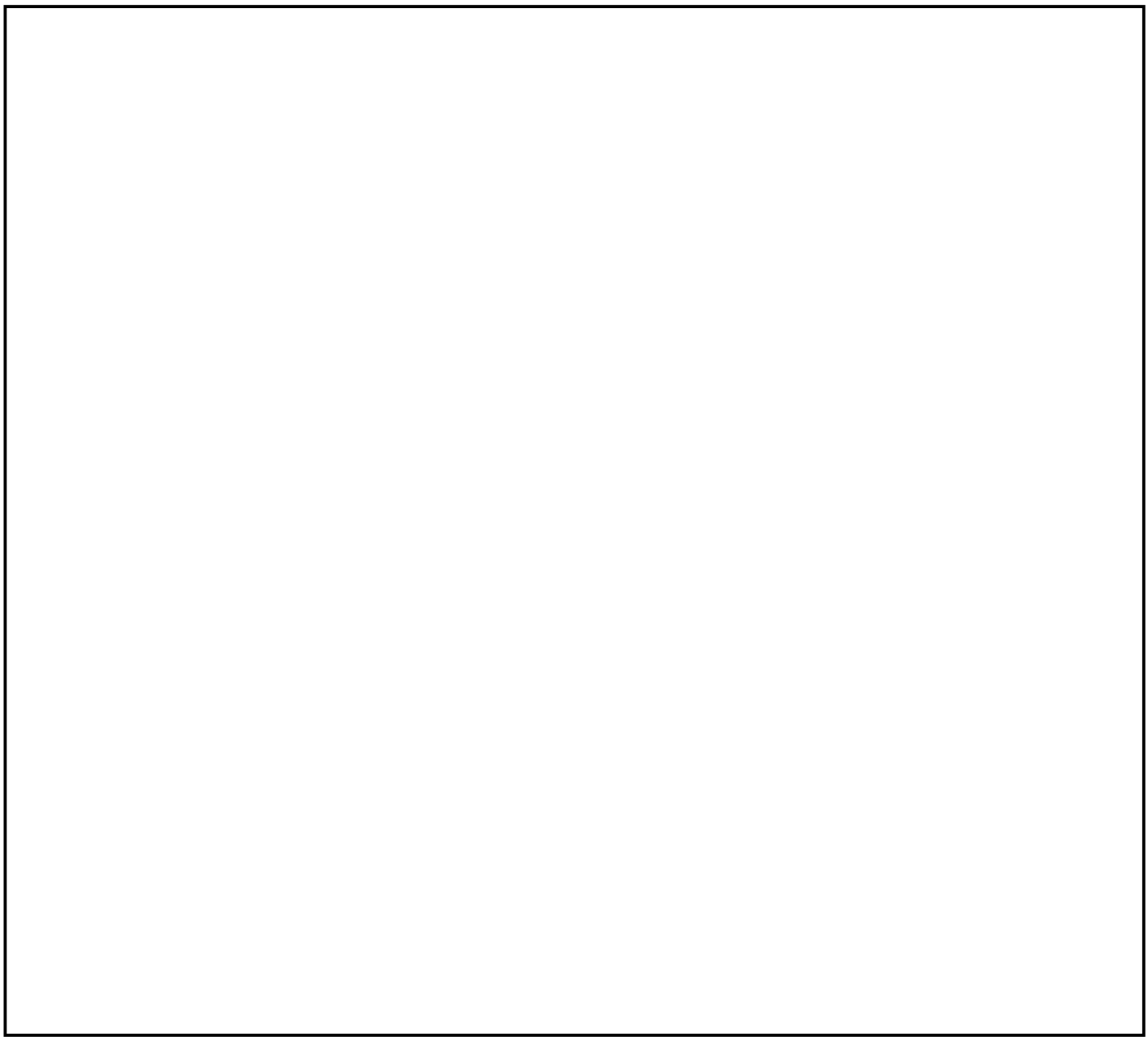
TO ALL FBI FIELD OFFICES/IMMEDIATE/

[redacted]

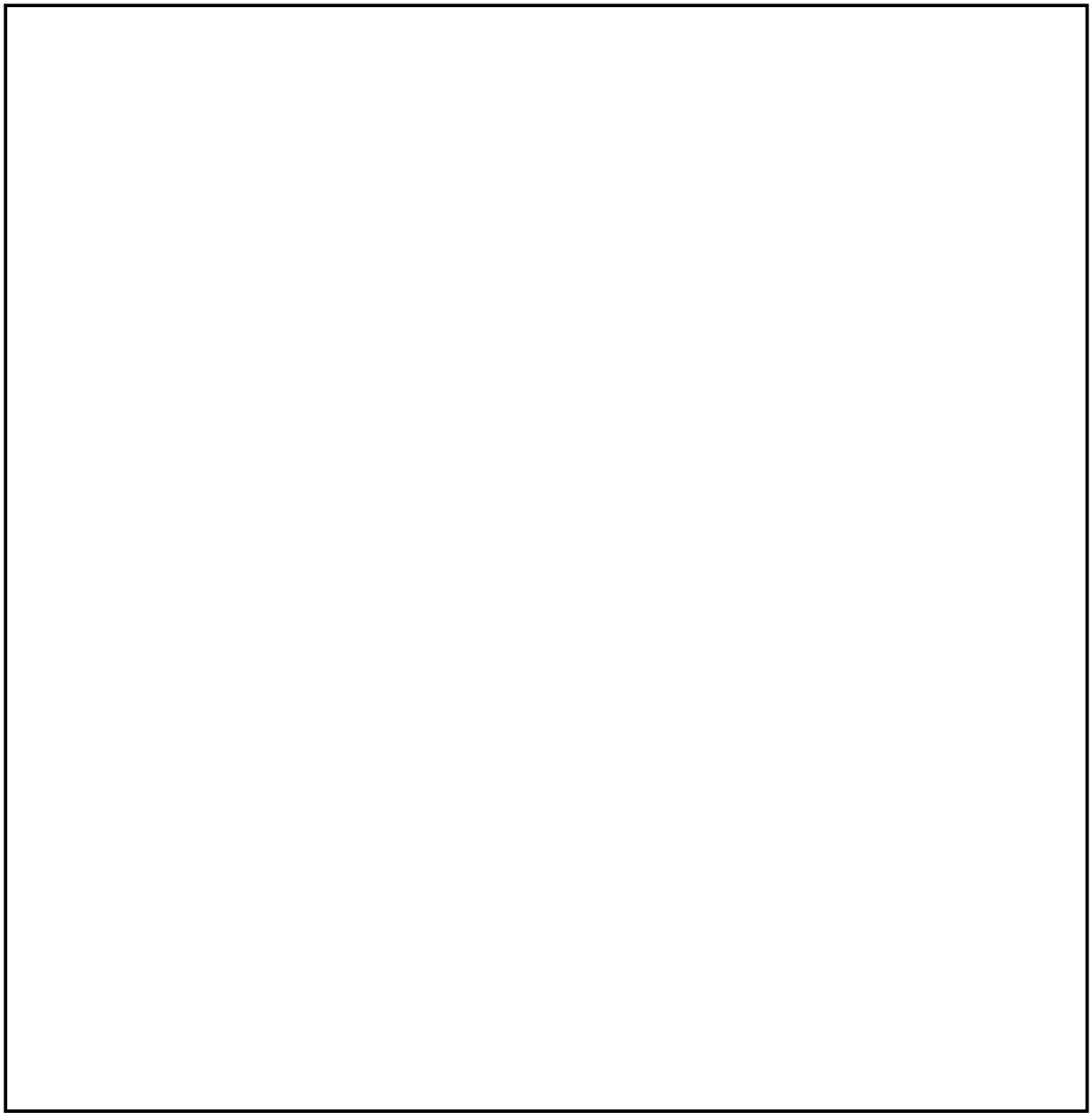
b7E

[redacted]

b7E



b7E



b7E

BT

UNCLAS E F T O FOR OFFICIAL USE ONLY

SECTION THREE OF THREE SECTIONS

CITE: //1301//

PASS: NIC WARNING STAFF TO NATIONAL WARNING COMMUNITY; JTF-CND APPROPRIATE DOD FACILITIES, SERVICE COMPONENTS AND TARGET LOCATIONS; NIPC TO FEDCIRC, CARNEGIE MELLON CERT.

SUBJECT: NIPC INFORMATION SYSTEM ADVISORY (NIPC ADVISORY 99-016).

TEXT CONTINUES:

6. (U) QUESTIONS AND REPORTS SHOULD BE DIRECTED TO THE NIPC WATCH & WARNING UNIT, CERT ORGANIZATIONS, AND LAW ENFORCEMENT PERSONNEL, AS APPROPRIATE. THE NIPC WATCH & WARNING UNIT CAN BE REACHED AT [redacted] (COMMERCIAL) OR [redacted] (CLASSIFIED) FROM 6AM TO 11PM WASHINGTON LOCAL TIME, OR E-MAIL AT [redacted]

b7E

BT

#0065

NNNN