

UNCLASSIFIED

VZCZCEIA845LGY471

PP RUCNFB

DE RUHPSGG #7277 0450319

ZNY SSSSS

P 140319Z FEB 98

FM USCINCPAC HONOLULU HI//J39//

TO RUEKJCS/JOINT STAFF WASHINGTON DC//J39/OPS//

INFO RUEKJCS/SECDEF WASHINGTON DC//ASD/C3I/DUSD(P)PS//

RUCJAAA/USCINCSUC MACDILL AFB FL//SUJ2/SOJ3/SUJ6//

RHCUAAA/USCINCTRANS CAT SCOTT AFB IL//J2/J3/J6//

RUHPSGG/USCINCLANT NORFOLK VA//J2/J3/J6//

RJCUSTR/USCINCSTRAT OFFUTT AFB NE//J2/J3/J6//

RJPEJNA/USCINCSPACE PETERSON AFB CO//SCJ2/SCJ3/SCJ6//

RJFGNDA/USCINCEUR VAIHINGEN GE//ECJ2/ECJ3/ECJ6//

RJCJACC/USCINCCENT MACDILL AFB FL//CCJ2/CCJ3/CCJ6//

RJMIAAAA/USCINCSU MIAMI FL//J2/J3/J6//

RHHHAAA/CINCPACFLT PEARL HARBUR HI//N2/N3/N6//

RJHVPAC/HQ PACAF HICKAM AFB HI//IN/DO/SC//

RUHEHMS/CUMMARFORPAC//G2/G3/G6//

RUEAHIC/CDRUSARPAC FT SHAFTER HI//APJPS/APIAS//

RHHJRAP/USARPAC INTEL FT SHAFTER HI//APIN//

20-110-126150-229

RJAGAAA/CUMUSOKREA SEUUL KOR//FK-J2/FK-J3/FK-J6//

RUALSFJ/COMUSJAPAN YOKOTA AB JA//J2/J3/J6//

RUWMHGA/ALCOM ELMENDORF AFB AK//J2/J3/J6//

Declassified by HQ USPACOM J06
Date Declassified: 6 Nov 2014
Authority: E.O. 13526

(1)

UNCLASSIFIED

UNCLASSIFIED

PAGE 02 RUHPSGG7277 ~~SECRET REL UK/CAN/AUS~~

RHHMUNS/COMSOPAC HONOLULU HI//SOJ2/SUJ3/SOJ6//

RJETIAA/NSACSS FT GEORGE G MEADE MD//NSUC/I3/SIPO/V15//

RJCNFB/FBI WASHINGTON DC//CITAC//

RUEAIIA/CIA WASHINGTON DC//CTG/DI/OTI/IWT//

RUEKDIA/DIA WASHINGTON DC//TWI/DS/J2J/SY/DAJ2A//

RJEJDCA/DISA WASHINGTON DC//D2/U3/D6/GOSC//

RJHDPAC/NCPAC HONOLULU HI//F4/F405//

RHHJAA/JICPAC HONOLULU HI//D1W/D5//

RUHHAAA/DISA PAC WHEELER AAF HI//PAC-ASSIST/PC6//

RJQVKEW/AFIWC KELLY AFB TX//CC/EA/EAC/OSK/IR//

RUDHIWA/DIRLIWA FT BELVUIR VA//ACERI/DR/DD//

RJCBFAD/FLTIN=OWARCEN NORFOLK VA//N2/N3/N6/SCIO/CISU//

RJLKGXA/NAVIN=OWARACT FT GEORGE G MEADE MD//N3//

RUQVKJW/JC2WC SAN ANTONIO TX//DR/DV/OP/PD//

RJETKEL/IUTC FT GEORGE G MEADE MD//AAG//

RJHPSAA/NCTAMS PAC HONOLULU HI//N3/N6//

RHHMUNA/USCINCPAC HONOLULU HI//J2/J3/J39/J6//

BT

~~SECRET REL UK/CAN/AUS~~

MSGID/GENADMIN/J-39/FEB 98//

UNCLASSIFIED

UNCLASSIFIED

PAGE 03 RUHPS3G7277 ~~SECRET REL UK~~

SUBJ/USPACOM CONSOLIDATED INFOSEC GUIDANCE FOR UNUSUAL COMPUTER
INTRUSION ACTIVITY//

REF/A/JOINT STAFF MSG DTG 131850Z FEB 98, SUBJ: HEIGHTENED
INFORMATION SYSTEMS SECURITY//

RMKS/1. ~~(S/REL UK/CAN/AUS)~~ A STRONG INFORMATION SYSTEMS SECURITY
POSTURE IS VITAL TO FULLY SUPPORT DAY-TO-DAY AND CONTINGENCY
OPERATIONS WITHIN THE PACIFIC THEATER. TO ENSURE ALL USPACOM
COMMANDS HAVE ACHIEVED AND ARE MAINTAINING SUCH A POSTURE, IN
ADDITION TO REQUIREMENTS LISTED IN REF A, ACCOMPLISH THE FOLLOWING
ACTIONS, IF NOT ALREADY COMPLETED:

A. ~~(S/REL UK/CAN/AUS)~~ THE CURRENT STATUS IS SUSPECT. INSTALL CURRENT
SECURITY PATCHES. SECURITY PATCHES CAN BE DOWNLOADED FROM

(b) (3) 10 USC § 130e

ENSURE THE

MOST CURRENT PATCHES FOR YOUR OPERATING SYSTEM ARE INSTALLED.

B. ~~(S/REL UK/CAN/AUS)~~ SPECIFICALLY FOR USERS ON THE SOLARIS 2.4
OPERATING SYSTEM, REVIEW DATE/TIME STAMP OF ALL **(b) (3) 10 USC § 130e**

TO ENSURE THE INSTALL DATES ARE CONSISTENT WITH SYS ADMIN ACTIVITY.

C. ~~(S/REL UK/CAN/AUS)~~ RUN CRACK AGAINST THE PASSWORD FILES ON ALL
FILE SERVERS N/DR YP/NIS SERVERS. CHANGE PASSWORDS FOR THOSE THAT
CAN BE EASILY CRACKED.

UNCLASSIFIED

UNCLASSIFIED

PAGE 04 RUHPSGG7277 S E C R E T REL UK

D. ~~(S/REL UK/CAN/AUS)~~ REQUEST NETWORK CONTROL CENTERS TAKE AN ACTIVE ROLE IN REVIEWING LOCAL INTRUSION DETECTION SYSTEM TRAFFIC TO ENSURE QUICKEST REACTION POSSIBLE TO SUSPICIOUS AND/OR MALICIOUS NETWORK ACTIVITY. VIGILANTLY REPORT INFORMATION OF THIS NATURE IAW THEATER NETWORK INCIDENT REPORTING PROCEDURES.

E. ~~(S/REL UK/CAN/AUS)~~ ALL SITES WITH (b) (3) 10 USC § 130e, 18 USC § 798(a) SYSTEMS CAREFULLY SCRUTINIZE THEIR SYSTEM AUDIT LOGS FOR UNUSUAL ACTIVITY. (b) (3) 10 USC § 130e, 18 USC § 798(a)

(b) (3) 10 USC § 130e, 18 USC § 798(a)

F. ~~(S/REL UK/CAN/AUS)~~ EXAMINE LOCAL NETWORKS TO ENSURE USER ACCESS, SYSTEM ROOT ACCESS AND DIAL-IN OR REMOTE ACCESS HAVE NOT BEEN ALTERED OR COMPROMISED. CHANGE OF PASSWORDS, ESPECIALLY ROOT PASSWORDS, IS HIGHLY RECOMMENDED AT THIS TIME. REMOTE MAINTENANCE ACCESS, AS WELL AS OTHER TYPES OF REMOTE ACCESSES, SHOULD BE SCRUTINIZED AND MINIMIZED WHERE POSSIBLE.

G. (S/REL UK/CAN/AUS) (b) (3) 10 USC § 130e, 18 USC § 798(a)

(b) (3) 10 USC § 130e, 18 USC § 798(a) REVIEW NETWORK SERVICES THAT SHOULD NOT BE ALLOWED INTO YOUR NETWORK FROM OFF-INSTALLATIONS AND BLOCK SERVICES APPROPRIATELY.

H. ~~(S/REL UK/CAN/AUS)~~ INSTALL SHADOWED PASSWORD FILES (IF

UNCLASSIFIED

UNCLASSIFIED

PAGE 05 RUHPSSG7277 ~~SECRET REL UK~~

AVAILABLE).

I. ~~(S/REL UK/CAN/AUS)~~ (b) (3) 10 USC § 130e, 18 USC § 798(a)

(b) (3) 10 USC § 130e, 18 USC § 798(a)

J. ~~(S/REL UK/CAN/AUS)~~ ENSURE ALL SYSTEMS HAVE AN APPROVED WARNING BANNERS. THIS IS REQUIRED IN THE EVENT THAT LEGAL ACTIONS ARE REQUIRED.

K. ~~(S/REL UK/CAN/AUS)~~ ACTIVITY FROM .MIL AND .GOV SHOULD ALSO BE REVIEWED. DO NOT ASSUME TRUSTED RELATIONSHIPS EXIST.

L. ~~(S/REL UK/CAN/AUS)~~ CHECK FOR THE EXISTENCE OF THE FOLLOWING

FILES: **(b) (3) 10 USC § 130e, 18 USC § 798(a)**

(b) (3) 10 USC § 130e, 18 USC § 798(a)

M. ~~(S/REL UK/CAN/AUS)~~ INCREASE OPSEC AWARENESS WITH SENSITIVITY TO WHAT IS PLACED ON THE NIPRNET. REMINDER: SENSITIVE INFORMATION SHOULD NOT BE TRANSMITTED OVER THE NIPRNET.

N. ~~(S/REL UK/CAN/AUS)~~ **(b) (3) 10 USC § 130e, 18 USC § 798(a)**

(b) (3) 10 USC § 130e, 18 USC § 798(a)

(b) (3) 10 USC § 130e, 18 USC § 798(a) LOOK FOR EVIDENCE OF A SIMILAR ATTACK BY CHECKING IF THE STATD PATCH HAS BEEN CHANGED SINCE 3 FEB 98.

O. ~~(S/REL UK/CAN/AUS)~~ REVIEW OPTIONS, AND OPERATIONAL IMPACTS LF,

UNCLASSIFIED

UNCLASSIFIED

PAGE 06 RUHPSGG7277 ~~SECRET REL UK~~

DISCONNECTING ALL BRIDGES BETWEEN UNCLASSIFIED AND CLASSIFIED NETWORKS, SUCH AS SECURE MAIL GUARD (SMG) BETWEEN UNCLASSIFIED AND SECRET LANS.

2. (U) POINTS OF CONTACT: NORMAL DUTY HOURS, POC IS (b) (6)
(b) (6), COMM (808) 477-4221. AFTER DUTY HOURS, CONTACT THE CDU AT DSN
477-722711

CLBY: RADM MOBLEY, J-3; REASON: 1.5(A); DECLON: 8 FEB 08

BT

#7277

NNNN

0146 00240/045 P15 0450526

UNCLASSIFIED