

**UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION**

BEFORE THE PRE-LICENSE APPLICATION PRESIDING OFFICER BOARD

In the Matter of)	Docket No. PAPO-00
)	
U.S. DEPARTMENT OF ENERGY)	ASLBP No. 04-829-01-PAPO
)	
(High Level Waste Repository: Pre-Application Matters))	

**EXHIBITS TO DEPARTMENT OF ENERGY'S RESPONSE TO THE PRE-LICENSE
APPLICATION PRESIDING OFFICER BOARD'S APRIL 19, 2007 ORDER**

On May 16, 2007, the Department of Energy filed its Response to the Pre-License Application Presiding Officer Board's April 19, 2007 Order. Attached are the exhibits referenced in the aforementioned pleading.

Respectfully submitted,

U.S. DEPARTMENT OF ENERGY

By Signed by Michael R. Shebelskie

Donald P. Irwin
Michael R. Shebelskie
Kelly L. Faglioni
HUNTON & WILLIAMS LLP
Riverfront Plaza, East Tower
951 East Byrd Street
Richmond, Virginia 23219-4074
Telephone: (804) 788-8200
Facsimile: (804) 788-8218
Email: dirwin@hunton.com
Of Counsel:

Martha S. Crosland
U.S. DEPARTMENT OF ENERGY
Office of General Counsel
Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585

Dated: May 17, 2007

May 17, 2007

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION
BEFORE THE PRE-LICENSE APPLICATION PRESIDING OFFICER BOARD

In the Matter of)	Docket No. PAPO-00
)	
U.S. DEPARTMENT OF ENERGY)	ASLBP No. 04-829-01-PAPO
)	
(High-Level Waste Repository: Pre-Application Matter))	

EXHIBITS TO DEPARTMENT OF ENERGY'S RESPONSE TO THE PRE-LICENSE
APPLICATION PRESIDING OFFICER BOARD'S APRIL 19, 2007 ORDER
CERTIFICATE OF SERVICE

I certify that copies of the foregoing EXHIBITS TO DEPARTMENT OF ENERGY'S RESPONSE TO THE PRE-LICENSE APPLICATION PRESIDING OFFICER BOARD'S APRIL 19, 2007 ORDER in the above captioned proceeding have been served on the following persons on May 17, 2007 by Electronic Information Exchange.

**U.S. Nuclear Regulatory Commission
Atomic Safety and Licensing Board
Panel**

Mail Stop - T-3 F23
Washington, DC 20555-0001

**Thomas S. Moore, Chair
Administrative Judge**

E-mail: PAPO@nrc.gov

Alex S. Karlin

Administrative Judge

E-mail: PAPO@nrc.gov

Alan S. Rosenthal

Administrative Judge

E-mail: PAPO@nrc.gov &
rsnthl@comcast.net

G. Paul Bollwerk, III

Administrative Judge

E-mail: PAPO@nrc.gov

Anthony C. Eitrem, Esq.

Chief Counsel

E-mail: PAPO@nrc.gov

James M. Cutchin

E-mail: PAPO@nrc.gov

Bethany L. Engel

E-mail: PAPO@nrc.gov

Jonathan Rund

E-mail: PAPO@nrc.gov

Susan Stevenson-Popp

E-mail: PAPO@nrc.gov

Bradley S. Baxter

E-mail: bxm@nrc.gov

Daniel J. Graser

LSN Administrator

E-mail: djg2@nrc.gov

ASLBP HLW Adjudication

E-mail:

ASLBP_HLW_Adjudication@nrc.gov

**U.S. Nuclear Regulatory Commission
Office of the Secretary of the
Commission**

Mail Stop - O-16 C1

Washington, DC 20555-0001

Hearing Docket

E-mail: hearingdocket@nrc.gov

Andrew L. Bates

E-mail: alb@nrc.gov

Adria T. Byrdsong

E-mail: atb1@nrc.gov

Emile L. Julian, Esq.

E-mail: eli@nrc.gov

Evangeline S. Ngbea

E-mail: esn@nrc.gov

Rebecca L. Giitter

E-mail: rll@nrc.gov

**U.S. Nuclear Regulatory Commission
Office of Congressional Affairs**
Mail Stop -O-17A3
Thomas R. Combs
E-mail: trc@nrc.gov

**U.S. Nuclear Regulatory Commission
Office of Public Affairs**
Mail Stop - O-2A13
David McIntyre
E-mail: dtm@nrc.gov

**U.S. Nuclear Regulatory Commission
Office of Nuclear Material Safety and
Safeguards**
Mail Stop - T-7 F3
Washington, DC 20555-0001
Jeffrey A. Ciocco
Email: jac3@nrc.gov

**U.S. Nuclear Regulatory Commission
Office of the General Counsel**
Mail Stop - O-15 D21
Washington, DC 20555-0001
Karen D. Cyr, Esq.
General Counsel
E-mail: kdc@nrc.gov
David A. Cummings, Esq.
E-mail: dac3@nrc.gov
Gwendolyn D. Hawkins
E-mail: gxh2@nrc.gov
Janice E. Moore, Esq.
E-mail: jem@nrc.gov
Trip Rothschild, Esq.
E-mail: tbr@nrc.gov
Harry E. Wedewer, Esq.
E-mail: hew@nrc.gov
Mitzi A. Young, Esq.
E-mail: may@nrc.gov
Marian L. Zabler, Esq.
E-mail: mlz@nrc.gov
OGCMailCenter
E-mail: OGCMailCenter@nrc.gov

**Egan, Fitzpatrick, Malsch & Cynkar,
PLLC**
Counsel for the State of Nevada
The American Center at Tysons Corner
8300 Boone Boulevard, Suite 340
Vienna, VA 22182
Robert J. Cynkar, Esq.

E-mail: rcynkar@nuclearlawyer.com
Joseph R. Egan, Esq.
E-mail: eganpc@aol.com
Charles J. Fitzpatrick, Esq.
E-mail: cfitzpatrick@nuclearlawyer.com
Jack Kewley
E-mail: jkewley@nuclearlawyer.com
Martin G. Malsch, Esq.
E-mail: mmalsch@nuclearlawyer.com
Susan Montesi
E-mail: smontesi@nuclearlawyer.com
Nakita Toliver
E-mail: ntoliver@nuclearlawyer.com

Nuclear Energy Institute
1776 I Street, NW, Suite 400
Washington, DC 20006-3708
Michael A. Bauser, Esq.
Associate General Counsel
E-mail: mab@nei.org
Ellen C. Ginsberg, Esq.
E-mail: ecg@nei.org
Rod McCullum
E-mail: rxm@nei.org
Steven P. Kraft
E-mail: spk@nei.org
Ann W. Cottingham
E-mail: awc@nei.org

**U.S. Department of Energy
Office of General Counsel**
1000 Independence Avenue, S.W.
Washington, DC 20585
Mary B. Neumayr, Esq.
E-mail: mary.neumayr@hq.doe.gov
Martha S. Crosland, Esq.
E-mail: martha.crosland@hq.doe.gov
Angela M. Kordyak, Esq.
E-mail: angela.kordyak@hq.doe.gov

U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, DC 20585
Eric Knox
**Associate Director, System Operations
and External Relations, OCRWM**
E-mail: eric.knox@hq.doe.gov
Dong Kim
LSN Project Manager, OCRWM
E-mail: dong.kim@rw.doe.gov

U.S. Department Of Energy
Office of General Counsel
1551 Hillshire Drive
Las Vegas, NV 89134-6321
George W. Hellstrom
E-mail: george.hellstrom@ymp.gov

Hunton & Williams LLP
Counsel for the U.S. Department of Energy

Riverfront Plaza, East Tower
951 East Byrd Street
Richmond, VA 23219
W. Jeffery Edwards, Esq.
E-mail: jedwards@hunton.com
Kelly L. Faglioni, Esq.
E-mail: kfaglioni@hunton.com
Melissa Grier
E-mail: mgrier@hunton.com
Donald P. Irwin, Esq.
E-mail: dirwin@hunton.com
Stephanie Meharg
E-mail: smeharg@hunton.com
Edward P. Noonan, Esq.
E-mail: enoonan@hunton.com
Audrey B. Rusteau
E-mail: arusteau@hunton.com
Michael R. Shebelskie, Esq.
E-mail: mshebelskie@hunton.com
Patricia A. Slayton
E-mail: pslayton@hunton.com
Belinda A. Wright
E-mail: bwright@hunton.com

White Pine County
City of Caliente
Lincoln County
Jason Pitts
E-mail: idt@idtservices.com

Lander County Nuclear Waste Oversight Program
315 South Humboldt St.
Battle Mountain, NV 89820
Deborah Teske, Administrator
E-mail: dteske@landercounty.com

Intertech Services Corporation
(for Lincoln County)
P.O. Box 2008
Carson City, NV 89702-2008

Dr. Mike Baughman
E-mail: bigboff@aol.com

Environment Protection Agency
Ray Clark
E-mail: clark.ray@epa.gov

Public Citizen
215 Pennsylvania Ave, SE
Washington, DC 20003
Michele Boyd, Legislative Representative
Critical Mass Energy and Environment
E-mail: mboyd@citizen.org

Senator Harry Reid
Attn: Sandra Schubert
Room 528 Hart Senate Office Building
United States Senate
Washington, DC 20510-2803
Email: sandra_schubert@reid.senate.gov

Abby Johnson
617 Terrace St.
Carson City, NV 89703
E-mail: abbyj@qbis.com

National Congress of American Indians
1301 Connecticut Ave. NW - Second floor
Washington, DC 20036
Robert I. Holden, Director
Nuclear Waste Program
E-mail: robert_holden@ncai.org

Ross, Dixon & Bell
2001 K Street N.W.
Washington D.C. 20006-1040
William H. Briggs
E-mail: wbriggs@rdbl.com

Churchill County (NV)
155 North Taylor Street, Suite 182
Fallon, NV 89406
Alan Kall
E-mail: comptroller@churchillcounty.org

State of Nevada (NV)
100 N. Carson Street
Carson City, NV 89710

Marta Adams

E-mail: maadams@ag.state.nv.us

Lander, Churchill and Mineral County

P. O. Box 33908

Reno, NV 89533

Loren Pitchford, LNS Administrator for Lander

E-mail: lpitchford@comcast.net

Talisman International, LLC

1000 Potomac St., NW

Suite 300

Washington, D.C. 20007

Patricia Larimore

E-mail: plarimore@talisman-intl.com

Inyo County (CA) Yucca Mtn Nuclear Waste

Repository Assessment Office

Chris Howard

GIS/LAN Administrator

Inyo County

163 May St.

Bishop, CA 93514

E-mail: choward@inyowater.org

Nuclear Waste Technical Review Board

Victoria Reich

E-mail: reich@nwtrb.gov

White Pine County (NV) Nuclear Waste Project Office

959 Campton Street

Ely, NV 89301

Mike Simon, Director

(Heidi Williams, Adm. Assist.)

E-mail: wpnucwst1@mwpower.net

Inyo County (CA) Yucca Mtn Nuclear Waste

Repository Assessment Office

P.O. Drawer L

Independence, CA 93526

Andrew Remus, Project Coordinator

E-mail: aremus@qnet.com

Nye County (NV) Department of Natural Resources & Federal Facilities

1210 E. Basin Road, Suite 6

Pahrump, NV 89048

David Swanson

E-mail: dswanson@nyecounty.net

Nye County (NV) Regulatory/Licensing Adv.

18160 Cottonwood Rd. #265

Sunriver, OR 97707

Malachy Murphy

E-mail: mrmurphy@cmc.net

Nuclear Waste Project Office

1761 East College Parkway, Suite 118

Carson City, NV 89706

Robert Loux

E-Mail: bloux@nuc.state.nv.us

Steve Frishman, Tech. Policy Coordinator

E-mail: steve.frishman@gmail.com

Nevada Nuclear Waste Task Force

Alamo Plaza, 4550 W. Oakley Blvd., Suite 111

Las Vegas, NV 89102

Judy Treichel, Executive Director

E-mail: judyntwf@aol.com

Yucca Mountain Project, Licensing Group,

DOE/BSC

Jeffrey Kriner

E-mail: jeffrey_kriner@ymp.gov

Lincoln County (NV) Nuclear Oversight Prgm

100 Depot Ave., Suite 15; P.O. Box 1068

Caliente, NV 89008-1068

Lea Rasura-Alfano, Coordinator

E-mail: jcciac@co.lincoln.nv.us

Mineral County (NV) Board of County Commissioners

P.O. Box 1600

Hawthorne, NV 89415

Linda Mathias, Administrator

Office of Nuclear Projects

E-mail: mineral@oem.hawthorne.nv.us

Eureka County (NV) Yucca Mtn Info Ofc

P.O. Box 990

Eureka, NV 89316

Laurel Marshall, Program Coordinator

E-mail: ecmarshall@eurekanv.org

**Counsel to Eureka County and Lander
County, Nevada**

1726 M Street N.W., Suite 600
Washington, D.C. 20036

Diane Curran

E-mail: dcurran@harmoncurran.com

**Clark County (NV) Nuclear Waste
Division**

500 S. Grand Central Parkway
Las Vegas, NV 89155

Irene Navis

E-mail: iln@co.clark.nv.us

Engelbrecht von Tiesenhausen

E-mail: evt@co.clark.nv.us

U.S. DEPARTMENT OF ENERGY

By Signed by Michael R. Shebelskie

Donald P. Irwin
Michael R. Shebelskie
Kelly L. Faglioni
HUNTON & WILLIAMS
Riverfront Plaza, East Tower
951 East Byrd Street
Richmond, Virginia 23219-4074
Telephone: (804) 788-8200
Facsimile: (804) 788-8218
Email: dirwin@hunton.com

Of Counsel:

Martha S. Crosland
U.S. DEPARTMENT OF ENERGY
Office of General Counsel
Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585

EXHIBIT A



NOFORN (UNCLASSIFIED; Enclosure (1) body removed)

DEPARTMENT OF THE NAVY

NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-0001

08V:DST:dst
NAVSEAINST 5511.32C
Ser 08V/05-01154
26 July 2005

NAVSEA INSTRUCTION 5511.32C

From: Commander, Naval Sea Systems Command

Subj: **SAFEGUARDING OF NAVAL NUCLEAR PROPULSION INFORMATION (NNPI)**

- Ref: (a) CG-RN-1, Rev. 3, DOE-DOD Classification Guide for the Naval Nuclear Propulsion Program (NOTAL)
(b) SECNAVINST 5510.36, Department of the Navy Information Security Program (ISP) Regulation
(c) NAVSEAINST 5230.12, Release of Information to the Public
(d) NAVSEAINST 5510.2B, Physical Security, Access and Movement Control at Shore Activities
(e) DOD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations
(f) NAVSEA S9213-45-MAN-000(N) Naval Nuclear Material Management Manual

- Encl: (1) Definition of U.S. Naval Nuclear Propulsion Information
(2) Naval Nuclear Propulsion Information Marking Requirements
(3) Protection Requirements for Electronic Processing of Naval Nuclear Propulsion Information
(4) Requirements for Contractors and Subcontractors
(5) Requirements for Visits to Naval and Commercial Facilities Performing Naval Nuclear Propulsion Work

1. Purpose. To promulgate the official U.S. Navy definition of Naval Nuclear Propulsion Information (NNPI) and to identify disclosure policies, safeguarding requirements and disposal requirements for documents or equipment containing such information. This revision represents a substantial rewrite of this instruction and should be read in its entirety. Side-bars are not provided for individual changes.

~~NOFORN: This document is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with prior approval of the Naval Sea Systems Command.~~

NOFORN

2. Cancellation. NAVSEAINST C5511.32B of 22 Dec 1993, Safeguarding of Naval Nuclear Propulsion Information, is hereby superseded.

3. Background. The importance of U.S. naval nuclear-powered ships as a major deterrent to war emphasizes the need for rigid controls over information relating to naval nuclear propulsion. NNPI is an obvious target for intelligence organizations of nations seeking to develop, expand or advance nuclear capabilities, or to acquire valuable data on U.S. Navy technology and capabilities.

4. Terminology

a. DOE Unclassified Controlled Nuclear Information (DOE UCNI). DOE UCNI involves information protected under Section 148 of the Atomic Energy Act. One part of DOE UCNI includes information pertaining to the reactor plants of naval nuclear propulsion plants. Documents containing unclassified DOE reactor plant information may be marked with a DOE UCNI warning statement when they are sent to Navy activities. The protection requirements are the same as those for Unclassified NNPI (U-NNPI). Therefore, documents marked as DOE UCNI will be protected as U-NNPI. (Note that DOD UCNI relates solely to information regarding protection of Special Nuclear Material for weapons and does not include reactor plant information.)

b. Foreign Interest. Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or entity organized under the laws of any country other than the U.S. or its possessions; and any foreign national. Firms organized under the laws of the United States, regardless of potential foreign ownership, can receive contracts requiring access to U-NNPI if the firm formally agrees to protect the information.

c. Foreign National. For the purposes of this instruction, a foreign national is any person not a United States citizen or a United States national (born in Puerto Rico, American Samoa, Guam or the U.S. Virgin Islands). Non-U.S. citizens or non-U.S. nationals permanently residing in the United States are considered to be foreign nationals.

Individuals who are dual citizens (hold both a U.S. citizenship and the citizenship of some other country) shall have special controls. See Section 9.b below.

d. Naval Nuclear Propulsion Information. Naval Nuclear Propulsion Information is all information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities. Enclosure (1) provides a more detailed definition of NNPI, including a system-by-system breakdown.

e. Need-to-know. A determination by a person having assigned responsibility for protection of information or material that a proposed recipient's access to such information or matter is necessary in the performance of official or contractual duties of employment.

f. Representative of a Foreign Interest. For the purposes of this instruction a representative of a foreign interest is any person, regardless of citizenship, functioning (in an individual capacity or on behalf of any corporation, person, or government entity) as an official, representative, agent, or employee of a foreign interest. One exception is that U.S. citizens appointed by their U.S. employer to act as a representative in the management of a foreign subsidiary of a U.S. corporation will not be considered representatives of a foreign interest.

g. Restricted Data. A special type of classified information as defined in Section 11(w) of Public Law 83-703 (The Atomic Energy Act of 1954, as amended), as "... all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142."

5. Scope. The provisions of this instruction are applicable to all equipment, components, documents, drawings, computer media, audiovisual media, and any other media containing classified or unclassified NNPI. Additional regulations on protection of Classified NNPI are defined by references (a) and (b).

6. Marking Requirements. Special handling and disclosure restrictions for NNPI have been in effect since the inception of the Naval Nuclear Propulsion Program. Prior to 1986, the large majority of unclassified documents were not marked with special warning notices. With the enactment of federal statutes mandating protective measures for a range of sensitive military

technology, including NNPI, marking became necessary. The party possessing NNPI is responsible to comply with the disclosure restrictions set forth in this instruction, whether or not the documents containing NNPI are marked with a warning notice.

a. Prospective Marking Requirement. All documents containing NNPI issued subsequent to the date of this instruction shall be marked in accordance with this instruction. Applicable local instructions should address requirements for marking of electronic documents, including email. Documents marked in accordance with past versions of this instruction do not require any modification. When portions of unmarked documents are revised or replaced, those portions and the cover, index, and distribution pages shall be marked in accordance with this instruction. When an unmarked document is reissued in its entirety, all pages shall be marked in accordance with this instruction. An older, unmarked document containing U-NNPI need not be marked if it is simply being copied for internal use and not for reissuance. Prior to off-site release of unmarked documents, they shall be marked and handled in accordance with this instruction.

b. NNPI Markings and Distribution Statements. References (a) and (b) contain classification, downgrading or declassification markings for classified NNPI. Enclosure (2) summarizes the marking requirements for NNPI.

c. Paragraph and Portion Markings. Paragraph or portion markings are not required for classified or unclassified NNPI.

d. Photographs and Audio Visual Materials. Photographs and audio visual material will be marked consistent with the classification of the information in the photograph. Photographs of naval nuclear-powered ships or nuclear support facilities shall be handled in accordance with reference (c). Audio visual material containing NNPI shall be marked on the cover and case of each item, and at the beginning and end of each tape or reel.

7. Control and Storage of NNPI. Classified NNPI shall be controlled in accordance with reference (b). U-NNPI shall be controlled so that individuals without a need-to-know cannot obtain visual or physical access which would permit detailed examination. When in use by authorized personnel, U-NNPI documents are considered to be under the direct custody of the authorized individual who must prevent detailed visual or physical access by individuals who do not have the required need-to-know. When there is a potential for access by

unauthorized personnel, U-NNPI should be locked up (e.g., key lock).

a. Transmittal of NNPI. Classified NNPI will be transmitted in accordance with reference (b). Documents containing U-NNPI shall be transmitted or shipped in a single opaque envelope or wrapping, as a minimum. The outer wrapping or envelope shall not be marked in a manner that would reveal the contents of the envelope or package to unauthorized personnel.

b. Off-site Handling. U-NNPI may be removed from a site subject to local controls approved by the cognizant government office or Commanding Officer, which ensure information is protected consistent with the disclosure requirements of this instruction and the information is promptly returned when no longer needed off site.

c. Electronic Processing of NNPI. Transmission of NNPI unencrypted, over uncontrolled computer networks (i.e., Internet) is considered to be release to the public and is prohibited. Protection requirements for electronic processing of NNPI are identified in enclosure (3) and include computer networks as well as telecommunications equipment (land-line phones, cell phones, facsimile machines, etc).

d. Visits to Facilities Performing Naval Nuclear Propulsion Work. Requirements for visits to naval and commercial facilities performing naval nuclear propulsion work are addressed in reference (d) and enclosure (4).

8. Disclosure Policy. Access to classified NNPI shall be limited to only those individuals who have an established need-to-know and an appropriate security clearance. For classified NNPI that is also Restricted Data, a final government clearance is required for access. Access to U-NNPI requires a need-to-know for the performance of assigned work as determined by local cognizant authority. Any exception to this policy must have prior written approval from NAVAL SEA SYSTEMS COMMAND (NAVSEA) (08). Any changes in access policy from past actions should be identified to NAVSEA (08). Additional specific disclosure policies are outlined below:

a. Foreign Disclosure. Reference (e) prohibits release of NNPI, classified or unclassified, to foreign nationals or representatives of foreign interests except as made pursuant to an approved government-to-government agreement. Furthermore, releases to be made under such an agreement require approval from the Chief of Naval Operations (CNO) in each instance.

b. Disclosure of U-NNPI to Persons with Dual Citizenship. All persons with dual citizenship with a need to access U-NNPI must be reported to NAVSEA (08) prior to being provided U-NNPI.

c. Disclosure to Personnel in the Executive Branch of the U.S. Government. Disclosure of NNPI to personnel in the Executive Branch of the U.S. Government, except for those involved in the Naval Nuclear Propulsion Program, requires the approval of NAVSEA (08) in each instance. The fact that an individual is employed by a U.S. Government activity is not in itself sufficient justification for release of NNPI to that individual.

d. Disclosure Outside of the U.S. Government. Disclosure of NNPI outside of the U.S. Government, including U.S. industry, private individuals or other interests, except when required in the performance of U.S. Naval Nuclear Propulsion Program tasks, requires NAVSEA (08) approval in each instance.

e. Disclosure in Judicial or Administrative Proceedings. When access to NNPI is solicited as part of a judicial or administrative proceeding, NAVSEA (00L) shall be apprised to ensure that proper protective mechanisms are put in place to prevent unauthorized disclosure of the information. These mechanisms may include formal protective orders or legal filings, and may result in denial of access to NNPI if such access is judged to be inappropriate or unnecessary.

f. Special Requirements for Contractors and Subcontractors. These requirements are addressed in enclosure (5).

g. Unauthorized Release of NNPI. Any release of NNPI in violation of the disclosure policy outlined in paragraph 9 of this instruction shall be reported to NAVSEA (08).

9. Public Release. NNPI, classified or unclassified, shall not be disclosed in any manner which may result in direct or indirect release to the public. No public comment should be made which would confirm or deny whether NNPI has been inadvertently released to the public. Release of information which reaches the public is considered tantamount to foreign disclosure. Any proposed public release which may contain NNPI must be submitted to the NAVSEA (00D) for review in accordance with reference (c). NAVSEA (00D) will authorize release of the information once it has been determined that it contains no NNPI.

a. Documents Containing NNPI. Use of NNPI in documents with the potential for public release or uncontrolled distribution should be avoided. In cases where the usefulness of a document with the potential for public release requires reference to NNPI, the information should be removed from the body of the document and issued as a separate supplement or enclosure. The use of an enclosure for NNPI allows appropriate distribution of the document while maintaining control of non-releasable information. References to documents containing NNPI in journals and other publications available to foreign governments or to the public should also be avoided.

b. Information Concerning the Environment and Occupational Safety and Health. Environmental information and Occupational Safety and Health (OSH) information is not NNPI unless presented in such a way that it reveals information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities. Special care should be taken to avoid or minimize the inclusion of NNPI in documents that pertain to environmental or OSH matters since such documents are more likely to require public release. Other requirements, such as privacy protection, may apply to environmental or OSH information; therefore the absence of NNPI should not by itself be interpreted to authorize public release of this information.

10. Disposal of NNPI

a. Disposal of Unclassified Documents Containing NNPI. Disposal of unclassified documents containing NNPI shall ensure that the information is not easily retrievable. Disposing of documents in the same manner as classified documents is preferred. Recycling is authorized provided the documents are shredded to 2" width or less and shredded material is controlled until turned over to the recycler. Other proposals for recycling require approval from NAVSEA (08). Alternative disposal methods, to include commercial or public trash collection arrangements, which ensure an adequate degree of control during and after disposal must be approved by NAVSEA (08).

b. Disposal of Components and Equipment which Reveal NNPI

(1) Prior to disposal of components or equipment which reveal NNPI, all markings (such as stock number, nameplate data, Special Material Identification Code (SMIC), tags, stickers,

transfer documents, meter face markings, etc.) which associate the equipment or component with a nuclear propulsion plant application must be removed or obliterated. If after removal or obliteration of such markings the equipment or component would still reveal NNPI, the item shall be disposed of in the same manner as classified material.

(2) In view of stringent controls for the disposal of radioactive waste, and in order to minimize radiological work, nuclear propulsion plant components or equipment to be disposed of as radioactive waste need not have markings removed or obliterated.

(3) Unless specifically authorized by a SHIPALT or other NAVSEA correspondence, reactor plant components assigned 2S Cognizance, SMIC X1 National Stock Numbers, shall not be disposed of unless first sent to a designated naval shipyard in accordance with reference (f) for disposition by NAVSEA (08). When NAVSEA (08) desires to dispose of such a component, a formal scrap directive will be provided to the naval shipyard awaiting disposition.

(4) H Cognizance, Naval Inventory Control Point (NAVICP) managed SMIC X2, X3, X4, X5 or X6 material will be sent to NAVICP (Code 009) for disposal as directed by the NAVICP Item Manager. NAVICP (Code 009) will dispose of this material in accordance with NAVICP (Code 87) instructions. However, selected H cognizance SMIC X3 material items (e.g., resistors, capacitors, and hand tools) which are not procured to nuclear unique specifications and other items designated by NAVSEA may be disposed of locally as directed by NAVICP (Code 87). Further, NAVICP managed H Cognizance SMIC X2 chemicals and other SMIC X2 material may be disposed by naval shipyards as directed by NAVICP (Code 87).

(5) Disposition of unused but no longer required reactor plant equipment and components provided by NAVSEA (08) prime contractors as Government furnished equipment shall be in accordance with this instruction, reference (f) and specific instructions obtained from the NAVSEA (08) representative at the applicable prime contractor (NSTR or ANSTR).

(6) Disposal of shipyard facilities, support systems and equipment used in reactor plant work, shall meet the criteria for disposal in paragraphs 10.b.(1) and (2) of this instruction.

11. NNPI Control Officer (NNPICO). Each activity which routinely deals with NNPI shall designate a manager familiar with NNPI protection procedures as the NNPICO. Each activity will ensure that this individual is technically qualified or a technically qualified individual is available for consultation with the NNPICO as needed. It shall be this individual's responsibility to ensure that appropriate measures are established and enforced to control, and to prevent unauthorized access to or dissemination of, NNPI in accordance with this instruction. This individual will be given written authorization by the cognizant government office/Commanding Officer to determine if documents are correctly marked as NNPI (without review by NAVSEA).

12. Implementation

a. Addressees other than private shipyards shall advise NAVSEA 08 within 30 days of the date of this letter of any reason preventing implementation of this instruction and the date by which all provisions of this instruction will be met.

b. Supervisors of Shipbuilding, Conversion, and Repair (SUPSHIPS) should incorporate this instruction into existing contracts and into the VIRGINIA-class Master Index of Reference Documents where this can be done at no increase in contract price or delay in delivery. If implementation of this instruction will increase the price of or delay delivery under any contract, then this instruction should not be implemented without authorization from NAVSEA 08. In such cases, SUPSHIPS should obtain cost proposals to implement this instruction on existing contracts. NAVSEA 08 should be advised within 30 days of the date of this letter whether this instruction has been implemented, and if not, a date by when a proposal for implementation will be submitted.

13. Contractual Effect. The action taken by this letter is considered by the Government to be within the scope of existing contracts and therefore does not involve or authorize any delay in delivery or additional cost to the Government, either direct or indirect.

14. Inquiries. Inquiries concerning the security requirements contained herein shall be forwarded to Commander, Naval Sea Systems Command (08).

//S//

K. H. DONALD
Director, Naval Reactors

Distribution: (See next page)

Distribution:

SNDL

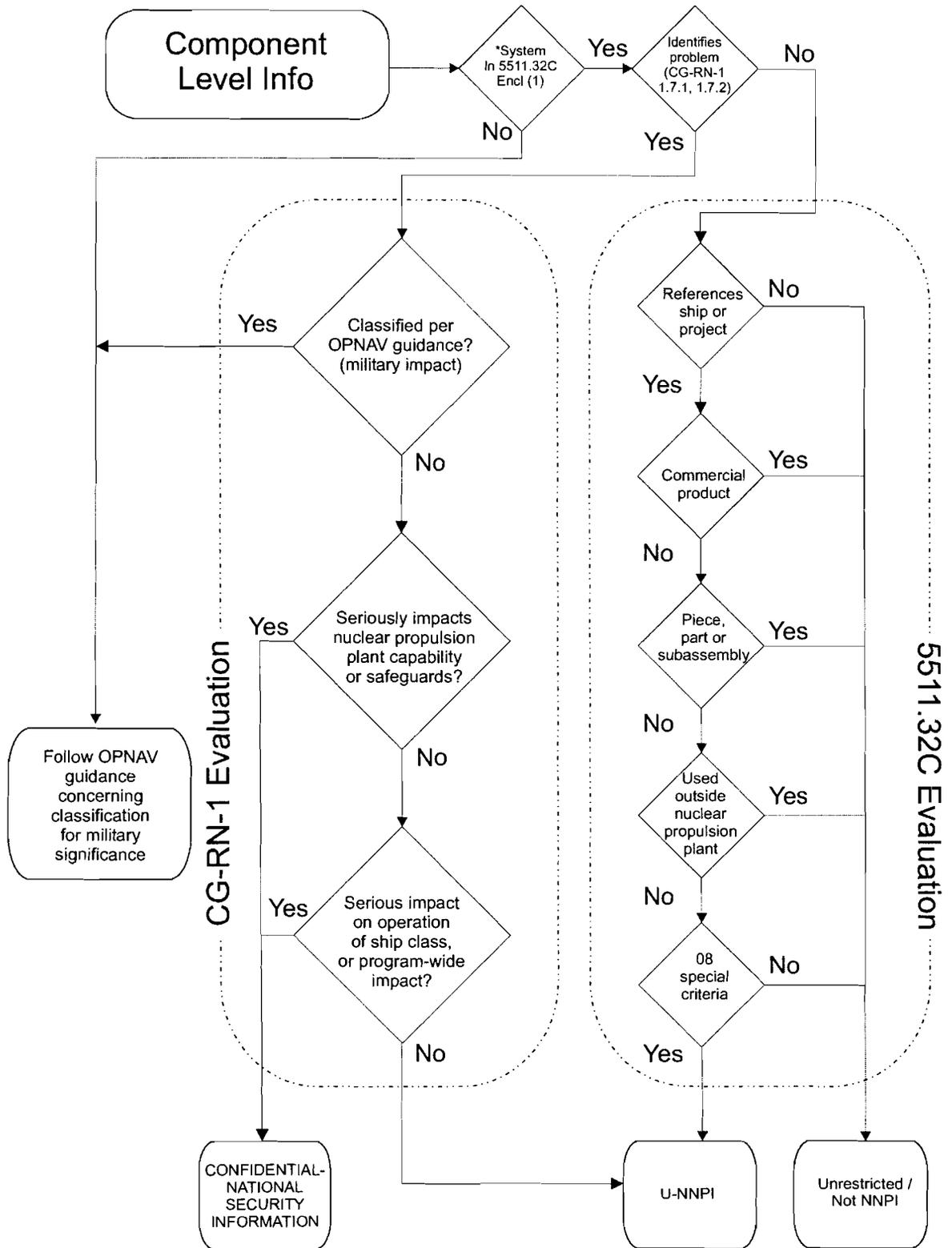
A1 Secretary of the Navy (ASN (IE), ASN (RDA), OGC)
A2A Department of the Navy Staff Offices (CHINFO, DONPIC, CNR, NCIS, and CIO)
A3 CNO (N2, N3/5, N4, N8, N09B, N09N, N76, N77, N86, N87, N88, N30N)
A5 Bureau of Naval Personnel
B1B SECDEF, Offices of the (ASD/ISA, ASD/PA)
B2A Defense Agencies (DISA, DIA, DTRA, DLA)
B2D DCMOR
B3 College and University (AFSC, NWC)
C7 U.S. Defense Attache Office
C58U Submarine Training Center Detachment
C84K Nuclear Power Training Unit Detachments
FA2 Network Warfare Command
FA10 Submarine Base, LANT
FA13 Submarine Support Facility
FA50 Trident Refit Facility, LANT
FB13 Submarine Base, PAC
FB29 Naval Intermediate Maintenance Facility, PACNORWEST
FF8 Board of Inspection and Survey
FKA1G Sea Systems Command, HQ
FKM9 Fleet and Industrial Supply Center (Norfolk, Pearl Harbor, Puget Sound, San Diego)
FKM14 NAVICP (Mechanicsburg)
FKM17 Supply Information Systems Activity
FKP7 Shipyard (10)
FKP8 SUPSHIP (Groton, Newport News, Puget Sound, San Diego)
FKP23 Nuclear Power Training Unit, SEASYSKOM
FKP26 SUBMEPP Activity
FS1 Office of Naval Intelligence
FT24 Fleet Training Center (Norfolk, San Diego)
FT27 Nuclear Power Training Unit, CNET
FT38 Submarine Training Center
FT53 Nuclear Power Training Command
FT54 Submarine School
FT85 Trident Training Facility
FT95 Submarine Training Facility
20A Fleet Forces Command
21A Fleet Commanders (COMPACFLT, COMLANTFLT only)
24A Air Force Commander
24A1 Air Force Commander, LANT
24A2 Air Force Commander, PAC
24G Submarine Force Commander
24G1 Submarine Force Commander, LANT

24G2 Submarine Force Commanders, PAC
26VV1 Submarine Force Shipyard Representative, LANT
(Groton, Newport News, Portsmouth NH)
26VV2 Submarine Force Shipyard Representative, PAC
(Bangor, San Diego, Puget Sound, Pearl Harbor)
28K Submarine Group, Squadron and Support Unit and
Center
29B Aircraft Carrier (CVN only)
29N Submarine (SSN)
29Q Fleet Ballistic Missile Submarine (SSBN)
29S Research Submarine (Nuclear) (NR)
32DD Submarine Tender (AS)
35 Historic Warship

Copy to:

SEA 104 (50)
SEA 08 (100)
Director, NMCI

Flow Chart for Component Level Information



NOFORN

NAVSEAINST 5511.32C

~~(UNCLASSIFIED WHEN SEPARATED FROM REMAINDER OF INSTRUCTION)~~

NAVAL NUCLEAR PROPULSION INFORMATION CONTROL

(Training Attachment)

This attachment is provided as a training guide that can be removed from the body of this instruction and provided to personnel/organizations to provide a better understanding of NNPI.

DEFINITION: Naval Nuclear Propulsion Information (NNPI) is defined as -

"information, classified or unclassified, concerning the design, arrangement, development, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear powered ships and prototypes, including the associated nuclear support facilities."

A more specific definition of NNPI and the requirements for safeguarding NNPI exists in NAVSEAINST 5511.32C, Safeguarding of NNPI of 26 July 2005. This document is approved by the Director, Naval Nuclear Propulsion Program (NNPP). Other specific requirements related to NNPI are in SECNAVINST 5510.30A, DoN Personnel Security Program Regulation and the Engineering Department Manual (EDM). SECNAVINST 5510.36, DoN Information Security Program Regulation refers to NAVSEAINST 5511.32C for matters related to NNPI.

CLASSIFIED NNPI: Classified NNPI consists of two types of information - Restricted Data (RD) and National Security Information (NSI). Authority to classify NNPI comes from two sources: (1) the Atomic Energy Act of 1954, as amended which governs RD, and (2) Presidential Executive Order (EO) 12958 of March 2003, as amended, which governs NSI.

Restricted Data

- The Atomic Energy Act covers information related to the use of special nuclear material. In the Naval Nuclear Propulsion Program (NNPP) this is information associated with the use of special nuclear material for the production of energy in the nuclear core.

NOFORN

~~(UNCLASSIFIED WHEN SEPARATED FROM REMAINDER OF INSTRUCTION)~~

~~(UNCLASSIFIED WHEN SEPARATED FROM REMAINDER OF INSTRUCTION)~~

- Per the Atomic Energy Act, access to RD requires an investigation on the character, associations, and loyalty of the individual requiring access and subsequent grant of a final Government security clearance.

National Security Information

- National Security Information (NSI), as defined in EO 12958, as amended, is classified information in the following categories, which if disclosed, could be expected to cause damage to national security:
 - military plans, weapons systems, or operations
 - foreign government information
 - intelligence activities, sources, or methods
 - foreign relations or foreign activities of the U.S.
 - scientific, technological, or economic matters relating to national security
 - U.S. government plans for safeguarding nuclear material or facilities
 - vulnerabilities relating or capabilities of systems or installations relating to national security

E.O. 12958, as amended, prescribes a uniform system for classifying, declassifying, and safeguarding NSI.

- NNPI that is classified NSI must be protected from disclosure to foreign nationals. Consequently, classified NNPI that is NSI is also marked and handled as NOFORN to require access only by cleared U.S. citizens with a need-to-know unless specifically authorized by NAVSEA (08).
- Personnel with an interim or final Government security clearance may access classified NNPI that is NSI.

UNCLASSIFIED NNPI (U-NNPI): U-NNPI is controlled and protected under one or more of the following: (1) the Atomic Energy Act of 1954, as amended, (2) the 1984 Defense Authorization Act, (3) Export Control Act Regulations of the Commerce Department, (4) Arms Export Control Act Regulations (i.e., International Traffic in Arms (ITAR); Munitions List), (5) Export of Sensitive Nuclear

~~(UNCLASSIFIED WHEN SEPARATED FROM REMAINDER OF INSTRUCTION)~~

NOFORN

NAVSEAINST 5511.32C

~~(UNCLASSIFIED WHEN SEPARATED FROM REMAINDER OF INSTRUCTION)~~

Information for Foreign Atomic Energy Regulations of the Energy Department.

- U-NNPI is information related to sensitive military technology (i.e., naval nuclear propulsion technology).
- Access to U-NNPI is limited to U.S. citizens with a need-to-know.
- No clearance is required for access to U-NNPI.
- U-NNPI is marked and handled as NOFORN.

3

Attachment (2) to
Enclosure (1)

NOFORN

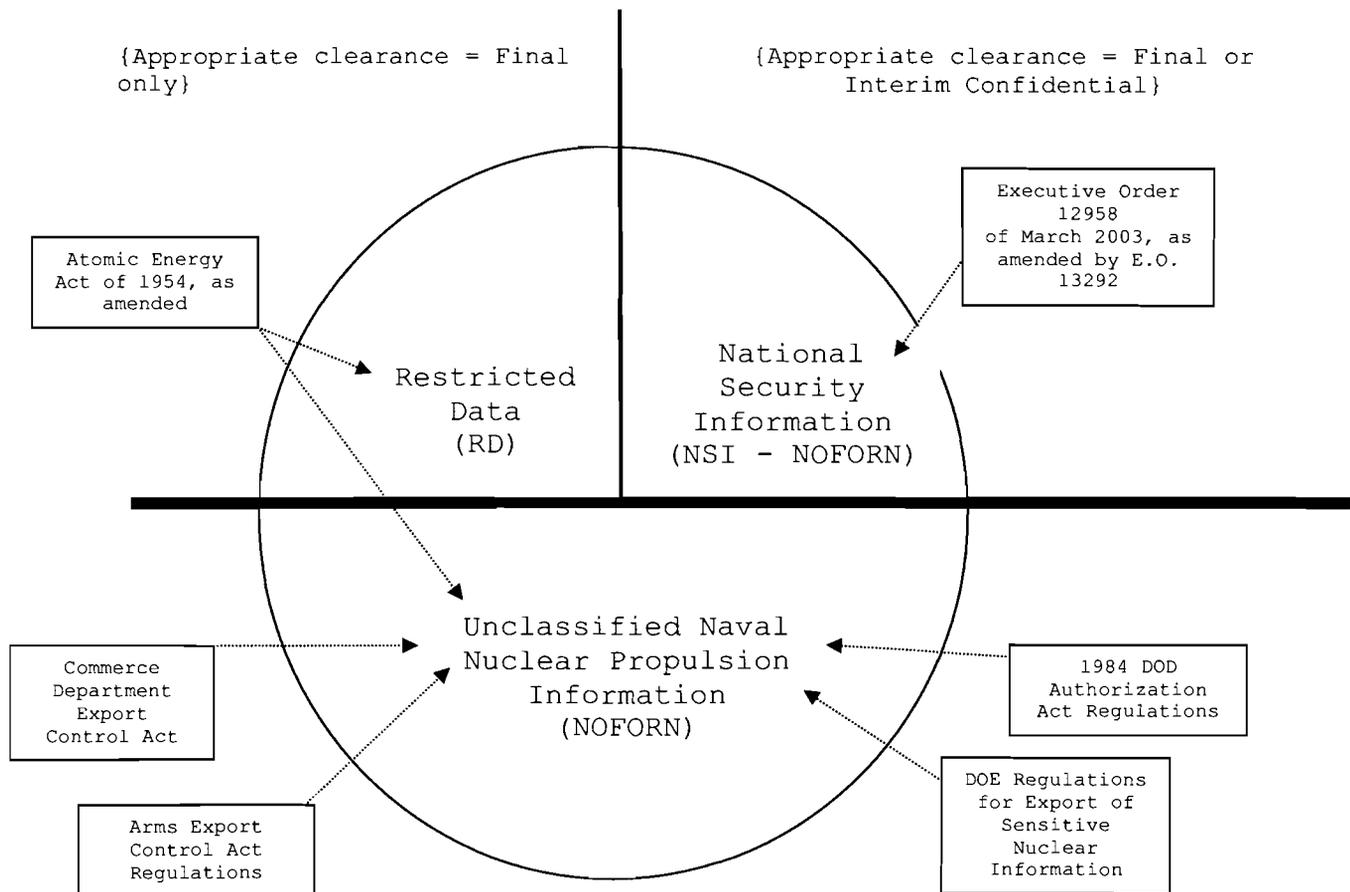
~~(UNCLASSIFIED WHEN SEPARATED FROM REMAINDER OF INSTRUCTION)~~

~~(UNCLASSIFIED WHEN SEPARATED FROM REMAINDER OF INSTRUCTION)~~

**NAVAL NUCLEAR PROPULSION
INFORMATION CONTROL**

**CLASSIFIED NAVAL NUCLEAR PROPULSION INFORMATION (NNPI) -
Secret or Confidential**

{Overall access requirements = U.S. citizenship +
"appropriate" clearance + need-to-know}



UNCLASSIFIED NAVAL NUCLEAR PROPULSION INFORMATION (U-NNPI)
{Overall access requirements = U.S. citizen + need-to-know}

~~(UNCLASSIFIED WHEN SEPARATED FROM REMAINDER OF INSTRUCTION)~~

NAVAL NUCLEAR PROPULSION INFORMATION MARKING REQUIREMENTS

1. For Naval Nuclear Propulsion Program documents containing CONFIDENTIAL RESTRICTED DATA (CRD)

CONFIDENTIAL RESTRICTED DATA (CRD)	
Cover page and/or First page	CONFIDENTIAL (stamp or large font, top and bottom) *Restricted Data Warning Notice (Bottom)
All other Pages (Top and Bottom)	CONFIDENTIAL (stamp or large font) (OPTIONAL) CONFIDENTIAL - RESTRICTED DATA

2. For Naval Nuclear Propulsion Program documents containing CONFIDENTIAL NATIONAL SECURITY INFORMATION (CNSI)

CONFIDENTIAL NATIONAL SECURITY INFORMATION (CNSI)	
Cover page and/or First page	CONFIDENTIAL (stamp or large font, top and bottom) *NSI Classification/Declassification Instructions (Bottom) *NOFORN Warning Notice (Bottom)
All other Pages (Top and Bottom)	CONFIDENTIAL (stamp or large font) (OPTIONAL) CONFIDENTIAL - NOFORN

3. For documents containing UNCLASSIFIED NAVAL NUCLEAR PROPULSION INFORMATION (U-NNPI)

UNCLASSIFIED NAVAL NUCLEAR PROPULSION INFORMATION (U-NNPI)	
Cover page and/or First page	NOFORN (stamp or large font, top and bottom) *NOFORN Warning Statement (Bottom)
All other Pages (Top and Bottom)	NOFORN (stamp or large font)

* The specific wording for these notices is identified on the following page.

"Distribution F" statements are not required for NNPI documents.

IDENTIFICATION OF THE WORDING FOR WARNING STATEMENTS

1. NOFORN Warning Statement:

NOFORN: This document is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with prior approval of the Naval Sea Systems Command.

2. Restricted Data Warning Notice:

Derived from: DOE-DOD Classification Guide
CG-RN-1 Rev. 3 dtd February 1996.

RESTRICTED DATA

This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.

3. National Security Information
Classification/Declassification Instructions:

Derived from: DOE-DOD Classification Guide
CG-RN-1 Rev. 3 dtd February 1996.

Declassify on: X2, X3, X6, X8.

This document shall not be used as a basis for derivative classification guidance.

THE FOLLOWING IS THE WORDING FOR DOE UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (DOE-UCNI) WHICH MAY BE RECEIVED BY THE SHIPYARD FROM DOE

Unclassified Controlled Nuclear Information.

Not for public dissemination. Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 USC 2168).

**PROTECTION REQUIREMENTS FOR ELECTRONIC PROCESSING OF NAVAL
NUCLEAR PROPULSION INFORMATION**

1. SCOPE

The Naval Nuclear Propulsion Program (NNPP) has the legal responsibility to protect Naval Nuclear Propulsion Information (NNPI). Classified and unclassified NNPI is shared across a wide range of Information Systems (IS) that are inherently vulnerable to exploitation and denial of service. Factors that contribute to the vulnerabilities include: increased reliance on commercial information technology and services; increased complexity and risk propagation through interconnection; the extremely rapid pace of technological change; and the relatively low cost of entry for adversaries.

This enclosure applies to all activities processing NNPI.

2. REFERENCE DOCUMENTS (Enclosure (3) only)

- a. Appendix III to OMB Circular A-130, "Management of Federal Information Resources" dated November 2000
- b. DOD Instruction 5200.40, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)" dated December 30, 1997
- c. DOD 8510.1-M, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual" dated July 31, 2000
- d. Assistant Secretary of Defense Memorandum, "Disposition of Unclassified DOD Computer Hard Drives" dated June 4, 2001
- e. DOD Directive 8500.1, "Information Assurance", October 24, 2002
- f. DOD Instruction 8500.2, "Information Assurance Implementation", February 6, 2003
- g. DOD Directive 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the DOD Global Information Grid (GIG)" dated April 14, 2003
- h. Naval Message, Chief of Naval Operations, 152315Z APR 2005, "Navy Operational Designated Approving Authority (DAA)"
- i. OPNAVINST 5239.1 (Series) "Navy Information Assurance (IA) Program"

j. SECNAVINST 5510.36, "Department of the Navy Information Security Program Regulation"

k. DOE Order 205.1, "Departmental Cyber Security Management Policy" dated March 21, 2003

l. DOE Guide 205.1-1, "Cyber Security Architecture Guidelines" dated March 8, 2001

m. DOE Notice 205.9, "Certification and Accreditation Process for Information Systems Including National Security Systems", dated February 19, 2004

n. DOE Notice 205.10, "Cyber Security Requirements for Risk Management", dated February 19, 2004

o. DOE Manual 471.2-2, "Classified Information System Security Manual", dated August 3, 1999

p. DOE Notice 205.12, "Clearing, Sanitizing, and Destroying Information System Storage Media, Memory Devices, and Other Related Hardware" dated February 19, 2004

q. DOE Notice 205.8, "Cyber Security Requirements for Wireless Devices and Information Systems" dated February 11, 2004

3. POLICY

Reference (a) requires Federal agencies to plan for security, ensure that appropriate officials are assigned security responsibility, and authorize system processing before starting operations and periodically thereafter. The documented technical and non-technical evaluation of an information system produces the necessary information required by the approving official to make a credible, risk-based decision on whether to place the system into operation. This process is known as certification. The Designated Approving Authority (DAA) is an official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority (Department of Energy (DOE) terminology). This authorization by senior Agency officials is referred to accreditation.

The certification and accreditation (C&A) process is designed to ensure that information systems processing U.S. Government information meet documented security requirements and will

continue to maintain the accredited security posture throughout the system life cycle. The process allows approving officials the flexibility to tailor the level of effort based on requirements for confidentiality (to protect information from unauthorized disclosure), integrity (to protect information against unauthorized modification or destruction) and availability (to assure reliable access to data by authorized users).

The primary objective of the security requirements for processing NNPI is to ensure that the features required by the Department of Defense (DOD) and DOE are applied to limit access to NNPI based on need-to-know controls.

As part of the C&A process mandated in reference (a), DOD and DOE require that when a site is developing an information system that will store, process and/or transmit classified or unclassified U.S. Government information, a security plan must be written to address all of the topics listed in the appropriate source guidance.

The system security plan should provide an explanation of how a system meets the requirements. If alternative protective measures are used to meet the intent of a specific requirement they must be documented in the system security plan. These methods must be documented in security plans for all new systems as well as when significant changes are made to existing accredited systems. Systems will be reaccredited whenever there is a change to the system that impacts its security posture or, at a minimum, every three years.

4. DEPARTMENTAL REQUIREMENTS

The following is provided to assist organizations that process NNPI (classified or unclassified) in following the applicable information security requirements for their Department (DOD or DOE). If any of these references are superseded by more current guidance, the more current guidance takes precedence.

a. DOD components, including facilities that are contracted by DOD organizations, must adhere to the guidance contained in references (b) through (j).

b. DOE organizations, including facilities that are contracted by a DOE organization, must adhere to the guidance contained in references (k) through (q).

c. Any organization that is not covered under DOD or DOE guidelines and has a need to process NNPI must first obtain

NAVSEA 08 approval. The mission of that organization will determine the source for guidance.

5. NNPP SPECIFIC REQUIREMENTS. While DOD and DOE requirements are sufficient to provide basic protections, this enclosure provides additional guidance for the protection of NNPI.

a. Preventing Access to NNPI by the Public, Foreign Nationals and Individuals or Organizations Without a Need-to-Know

1) Information systems processing classified or unclassified NNPI are required to prevent access by foreign nationals, representatives of a foreign interest, and the public, as well as individuals and/or organizations without a valid need-to-know. Exceptions require the specific approval of the cognizant DAA in consultation with NAVSEA 08Y.

2) Publicly accessible web pages and e-mail containing NNPP technical information that are made available or sent external to the activity must be treated as public disclosures, and therefore can contain no unencrypted NNPI. Public web pages related to the Naval Reactors program must be approved by NAVSEA 08.

3) Classified information systems processing NNPI must also employ need-to-know controls. For example, not every user of the Secret Internet Protocol Router Network (SIPRNET) has a need-to-know for NNPI. Do not rely solely on the classification of a system to grant access to NNPI.

4) Users of systems processing NNPI shall not permit individuals without a valid need-to-know to have access to the system while NNPI is being processed. For example, individuals without need-to-know shall not be permitted to interact with applications running under an authorized NNPI user's account. Incidental visual access to computer screens is not considered access to the system.

5) Personally owned computing systems, including, but not limited to, personal computers (PC), laptops, and Portable Electronic Devices (PED) such as Personal Digital Assistants (PDA), are not authorized for processing NNPI. Exceptions require the specific approval of the cognizant DAA and Naval Reactors (NR)/NAVSEA 08Y.

6) Sites establishing new video conferencing systems that are to be used to process U-NNPI, must use at a minimum, National Institute of Standards and Technologies (NIST) approved

Federal Information Processing Standards (FIPS) 140-2 level encryption. A National Security Agency (NSA) approved Type I encryption solution must be used on all video conferencing systems processing classified NNPI.

7) Care must be taken to prevent foreign national access to NNPI by means of land-line telephone conversations. U-NNPI may be discussed with U.S. citizens subject to need-to-know controls using land-line telephones without FIPS 140-2 encryption inside the continental U.S. and U.S. territories. However, U-NNPI voice communications via land-line telephones without FIPS 140-2 encryption to communicate with U.S. citizens (with a valid need-to-know) located outside the U.S. or U.S. territories is prohibited unless specifically approved by the cognizant DAA in consultation with NAVSEA 08.

8) All classified voice communications via land-line telephones must employ an NSA Type I encryption solution regardless of location.

9) Cellular telephones may be used to conduct U-NNPI voice communications within the U.S. and U.S. territories without FIPS 140-2 encryption. These unencrypted voice communications should only be used for short periods of time and only used in situations where land-line telephones are unavailable and the mission necessitates immediate voice communications.

10) All U-NNPI voice communications on cellular phones to/from locations outside the U.S. or U.S. territories must employ FIPS 140-2 or NSA Type I encryption.

11) All classified NNPI voice communications via cellular phones must employ an NSA Type I encryption solution regardless of location.

12) U-NNPI messages should not be left on any voice mail system.

13) Classified NNPI can only be transmitted on a secure facsimile (fax) machine employing an NSA Type I encryption solution regardless of location.

14) Land-line fax machines with volatile memory may be used to process U-NNPI without encryption inside the U.S. provided local procedures are in place to prevent access by foreign nationals and/or individuals without a valid need-to-know.

This guidance pertaining to fax machines with volatile memory may be applied to a fax machine in the residence of an employee with a valid need-to-know for U-NNPI. However, processing U-NNPI on a fax machine in a residence shall only occur to resolve emergent or time-sensitive issues where a delay until the next business day would have a significant negative impact on fleet support or business operations. DAAs authorizing U-NNPI faxes in a residential environment must incorporate the following minimum standards in local policies:

- a) Personally owned computers with built-in fax modems are prohibited from processing U-NNPI.
- b) U-NNPI shall be controlled so that access by individuals without a need-to-know, including foreign nationals is prevented.
- c) Fax machines processing U-NNPI shall not use ribbon based print mechanisms. Only print mechanisms that do not retain the image of the document (e.g., ink-jet, laser) are permitted.
- d) The government or contractor employee who owns the fax machine is the only individual authorized to transmit and/or receive a U-NNPI fax. That individual must be present at the fax machine when the U-NNPI is transmitted or received.
- e) Upon receipt of a U-NNPI fax, the sender and the recipient must confirm that the document was received in its entirety.
- f) Home fax numbers shall not be pre-programmed into Government or contractor owned fax machines.
- g) U-NNPI may not be duplicated in a residential environment and shall be controlled in accordance with the guidance contained in this instruction.
- h) U-NNPI documents must be returned to the work place for copying, long-term storage and/or destruction on the user's next normal work day.
- i) User Security Responsibility Acknowledgement forms shall be developed by the site to include the guidance contained in this instruction. These agreements must be signed by the user and the user's manager. The intent of the user manager signature is to validate the need to conduct U-NNPI business on a residential fax machine.

j) In the event that there is an emergent need to transmit a U-NNPI fax to a fax machine at a residence, and the recipient has not completed a User Security Responsibility Acknowledgment form, it is the sender's responsibility to verify with the recipient that the recipient meets the requirements set forth in this instruction. Immediately upon returning to work the next normal business day, the recipient shall notify their site Information Assurance Manager (IAM) (Information Systems Security Manager (ISSM) is the equivalent DOE position), Naval Nuclear Propulsion Information Control Officer (NNPICO) or designated alternate, that a U-NNPI fax was received. The recipient shall also be required to complete the User Security Acknowledgment form.

k) Inadvertent release, exposure or loss of NNPI shall be immediately reported to the site IAM, NNPICO or locally designated alternate.

l) The site IAM, NNPICO or other locally designated alternate shall maintain copies of all User Security Responsibility Acknowledgement forms for personnel under their cognizance.

15) Land-line fax machines with non-volatile memory may also be used to transmit U-NNPI without encryption inside the U.S. provided local procedures are in place to prevent access by foreign nationals or individuals without a valid need-to-know. Fax machines with non-volatile memory must be controlled as U-NNPI and secured appropriately. Fax machines with non-volatile memory are not authorized for processing U-NNPI in a residential environment.

16) Fax machines with wireless connections (in any environment) may not be used to process U-NNPI without first obtaining NAVSEA 08Y approval.

b. Administrative Controls

Any site that processes NNPI on an information system shall be defined as routinely handling NNPI and shall designate a NNPICO in accordance with Section 12 of this instruction.

The DAA is an official with the authority to formally assume responsibility for operating an IS at an acceptable level of risk.

(1) Navy:

(a) Reference (h) was issued to provide additional direction and guidance regarding the Operational DAA responsibilities of Commander Naval Network Warfare Command (COMNAVNETWARCOM) in advance of a revision to reference (i). Reference (h) defines an operational IT network as:

(1) A network that connects to the DOD Information System Network (DISN), this includes but is not limited to; Non-secure Internet Protocol Router Network (NIPRNET), Defense Research and Engineering Network (DREN), Secret Internet Protocol Router Network (SIPRNET), DISN Video Services (DVS), and Defense Red Switch Network (DRSN).

(2) All business and/or tactical systems currently in use that are operated by the Navy or by a contractor on behalf of the Navy, including but not limited to stand-alone systems and systems that use a commercial Internet Service Provider (ISP).

(3) Echelon II and their claimancy "Legacy" networks that have not transitioned to the Navy/Marine Corps Intranet (NMCI) or Outside the Continental United States Base Level Information Infrastructure (OCONUS BLII).

Echelon II Headquarters organizations may continue to function as the DAA over claimant "Legacy" networks that have not transitioned to NMCI or OCONUS BLII until expiration of current Interim Authority to Operate (IATO) or Authority to Operate (ATO), and anytime a new system or device is connected to the Navy operational network.

(b) Reference (h) authorizes the Commanding Officer of a U.S. Navy vessel operating at sea to perform the duties as a Deployed DAA. The Deployed DAA authority allows the Commanding Officer the flexibility to ensure system/network capabilities are maintained to meet the operational requirements of the assigned mission. The Deployed DAA must keep the operational DAA apprised of actions that deviate from the norm. When the afloat unit returns to port, all authority reverts to COMNAVNETWARCOM.

(2) Department of Energy (DOE):

The NR Information Systems Security (ISS) DAA is comprised of a group of Federal government managers at NAVSEA 08, Pittsburgh Naval Reactors (PNR) and Schenectady Naval Reactors (SNR). The NR ISS DAA accredits NNPI systems at DOE sites and/or sites that have principal contracts with DOE. This also includes systems

at other locations intended for the exclusive use of NR Program personnel (e.g. NRRO and RPCO offices).

The NNPP funds, operates, maintains, certifies and accredits the classified Naval Nuclear Propulsion Program Network (NNPP Net). NNPP Net security guidance can be obtained by contacting NAVSEA 08Y. The NNPICO for any site connected to the NNPP Net must work with local information security management and the local DAA to ensure complete compliance with the NNPP Network Security Policy. The NNPICO for the site shall notify their local information security management and local DAA of any issues or technical problems that impact compliance.

If any information system interconnects with an NR ISS DAA accredited system (e.g., NNPP Net) then the NR ISS DAA must approve the connection.

c. Physical Protection and Marking

1) Commensurate with the level of information processed, systems that contain NNPI are required to control physical access to the information technology resources in addition to providing software protections. These controls shall be in place to prevent unauthorized physical access, tampering, damage, and theft. This can be achieved by controlling access into specific areas or by controlling access to specific resources (e.g., PCs, printers, servers, network devices, wiring closets, etc).

2) Equipment and media must be marked to identify the highest level of information authorized for processing.

3) Classified media shall be marked (i.e., with a pen/marker) or labeled (via an affixed media label) with the appropriate classification level and include the proper warning statement identified in this instruction, where space permits. Media that contains U-NNPI shall be marked (i.e., with a pen/marker) or labeled (via an affixed media label) "NOFORN" and include the NOFORN warning statement identified in this instruction, where space permits. In those cases where the size or type of media does not support the application of Classification/NOFORN markings, the media shall be placed in a container that is marked with the appropriate level and includes the proper warning statements identified in this instruction.

4) When unattended, electronic media containing NNPI (classified or unclassified) must have adequate physical protections commensurate with the level of information they contain.

5) Ingress/egress controls for computer media and equipment shall be in accordance with local policy.

d. Network Controls

Data transmission of U-NNPI within a site can be accomplished without encryption provided the originating point, transmission lines, and the ending point are within the same site and properly controlled. (A "site" is that area within a facility's boundary, under the facility's control. A site can be as small as a single building or much larger, such as a shipyard or Naval Base.) If these conditions can not be met, the data in transit must be encrypted using FIPS 140-2 level encryption.

e. Configuration Guides

1) The National Security Agency (NSA), the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) have all developed and distributed security configuration guides for a wide variety of open source and proprietary software. These guides provide the best possible security options for the most widely used products. Sites designing systems to process NNPI are encouraged to utilize the appropriate NSA, NIST or CIS security configuration guides when practical.

2) The use of Standard Security Configuration (SSC) Guides for the NNPP Net is required. SSCs for the NNPP Net can be obtained through NAVSEA 08Y or the NNPP Net NSO at BPMI.

f. Disposal of Information Systems Equipment and Media

DAAAs should consider ways to reduce the amount of electronic media. For Navy facilities, reference (j) states, "Commanding Officers should establish at least one day each year as clean out day when specific attention and effort is focused on the disposition of unneeded classified and controlled unclassified information". Non-DOD organizations are strongly encouraged to adopt similar practices.

Special handling is required for disposal of equipment and media used in systems authorized to process NNPI.

1) Systems That Process Classified NNPI

All non-volatile user addressable memory materials must be removed from computing equipment that has been used to process classified NNPI and the materials must be degaussed or destroyed in accordance with NSA guidance for destruction of classified

material prior to disposal. This includes, but is not limited to, items such as computer hard drive platters, removable media such as floppy disks, Compact Disks (CDs) and Programmable Read Only Memory (PROM) (including electronic storage devices that are embedded in multi-function devices such as copiers/printers).

2) Systems That Process Only Unclassified NNPI (U-NNPI)

Electronic storage devices (computer hard drives, digital magnetic tapes, etc.) used to process information no higher than U-NNPI may be released outside the NR Program (for reuse, recycling, or disposal) only after the devices have been sanitized, degaussed, or destroyed in accordance with references (d) or (p).

The guidance provided in reference (d) for returning the hard drives of leased computers to suppliers without sanitizing, degaussing, or destruction does not apply to disks used for U-NNPI. The hard drives of leased computers (including electronic storage devices that are embedded in multi-function devices such as copiers/printers) processing U-NNPI must be sanitized, degaussed or destroyed prior to release to the vendor.

g. Connections to Internal and External **Unclassified** Networks

Internal networks are those contained entirely within the site. External networks are those with any component (client, server, network, or transmission equipment) that is located outside the site, that can be accessed from outside the site, or that can be used to access any information system that is outside the site.

1) Connections of U-NNPI Systems to Internal Networks:

Internal systems approved to process U-NNPI may be connected together with the approval of the cognizant DAA.

With the approval of the cognizant DAA, a system approved to process U-NNPI may be connected to an internal system that is approved to process other sensitive unclassified U.S. Government information, even though that system may not be approved for U-NNPI. These connections require the use of a firewall or other Controlled Interface (CI). The CI managing access between the systems must be located on-site. In addition, controls must be employed to ensure that U-NNPI is not transmitted to the system that is not approved for U-NNPI.

2) Connections of U-NNPI Systems to External U-NNPI Networks:

Access to any information system containing U-NNPI from off-site requires protection beyond that provided for access from within the site. Access between locations could result in the potential loss of access control by either location. Validation of U.S. citizenship and need-to-know for personnel at the other location is required.

U-NNPI systems must not be connected to systems that are external to the activity's site unless the external systems are approved to process U-NNPI. Any transmission of U-NNPI off-site must be encrypted using Federal Information Processing Standards (FIPS) 140-2 certified method (software or hardware) or NSA Type I encryption.

Before allowing users from an off-site location to access, (which must be from a U-NNPI system) the host information system must be configured to record the full audit trail of all actions taken by the off-site user and the off-site user must sign both NNPI user and non-disclosure agreements. The connecting information system must also meet the requirements for a U-NNPI system. No connections to U-NNPI systems shall be permitted to or from sites outside of the US without explicit NAVSEA 08 approval.

The security plan for the system must describe the protections in place to ensure users are unable to obtain access to systems processing U-NNPI from other than authorized locations.

a) Methods must be implemented to monitor and detect personnel attempting to gain unauthorized access to the system. In conjunction with monitoring and detection capabilities, the security plan will identify the process in place to respond to unauthorized access to the system. The use of Commercial-off-the-Shelf (COTS) Intrusion Detection packages on the network or on the host file server meets the requirement for monitoring access.

b) User agreements for access to the system must state that only equipment approved for the processing and storage of U-NNPI information may be connected. User agreements must also state that the connection of personally-owned computers or the use of standalone personally owned computers for processing and storage of U-NNPI is prohibited.

3) Use of External Networks at Sites That Have U-NNPI Approved Systems:

If sites with U-NNPI approved networks also have access to off-site systems not approved for U-NNPI such as the Internet, the off-site connections must be logically or physically isolated from any on-site system(s) that process U-NNPI. To ensure that U-NNPI information is not transmitted to such sites, the U-NNPI connections may only be approved for sites that have the following controls:

a) The system that the user resides on must employ an auditing capability to provide individual accountability for off-site access such as web addresses visited.

b) The system that the user resides on must also maintain an auditable copy of all E-mail messages (including attachments) sent off-site. These copies can be in the form of back-up tapes. These copies must be retained for a minimum of one year.

c) Ordinary users must not have the ability to alter or delete the audit trail or E-mail history.

d) A random sample audit of network traffic that goes off-site must be performed periodically to verify that no U-NNPI has been transmitted off site. The audit frequency, sample size, and policy for responding to findings should be approved by the cognizant DAA. All findings of unauthorized disclosure shall be reported to NAVSEA 08 in accordance with the guidance listed previously under administrative controls.

h. Controls on Transfer of Information from Classified Systems

1) DAAs must consider measures to control the removal of data from an information system where classified NNPI is processed. Such measures should provide positive controls for the prevention of unauthorized data removal. Examples of positive controls are:

a) The physical prevention of an ordinary user's ability to send information to output media devices (e.g., floppy drives, tape drives, etc.) and the physical prevention of ordinary users from connecting such devices to user accessible ports (e.g., use of approved hardware enclosures that enclose the CPU).

b) The logical prevention of an ordinary user's ability to send information to output media devices (floppy drives, tape drives, etc.) and the logical prevention of

ordinary users from connecting such devices to user accessible ports. Such logical prevention shall include the ability for system administrators/auditors to centrally manage and audit the logical controls.

2) There are occasions when information must be removed from an information system processing classified NNPI for the purpose of transferring the information to another system of lesser classification. In these situations, the cognizant DAA should establish controls to ensure the data is properly classified, marked and handled and that the transfer is justified. Such transfers should only be made where there is no connectivity between the source information system and destination system. Examples of these controls are:

a) A two-person review methodology (with provisions for one-person reviews for urgent or back shift transfers) that includes one person with an adequate level of training to determine the classification of the information.

b) Logging of all transferred information (manually or electronically). The log should include file name, reviewers, review times, file classification, and the time of the transfer. Copies of these logs should be maintained for a period of time as determined by the cognizant DAA and are subject to NAVSEA 08 review at any time.

c) Copies of the transferred data should be maintained for a period of time as determined by the cognizant DAA.

d) The cognizant DAA (or their designated representative) should establish a self-assessment program to ensure acceptable transfer practices are being followed. Copies of these assessments should be maintained for a period of time as determined by the cognizant DAA and are subject to NAVSEA 08 review at any time.

The above requirements are not intended to be applied to system backup media that supports restoring the system in the event of deletion, corruption and/or the archiving of that information for long term record keeping purposes.

3) A recommended implementation of these two-person controls is to use hardware Central Processing Unit (CPU) security enclosures and a centralized media transfer center methodology. This approach physically controls access to classified CPU I/O ports thus reducing the risk of attaching unauthorized devices. It also supports a centralized media

center methodology whereas a classification review can be conducted by a person knowledgeable in CG-RN-1 requirements before the information is transferred.

A two-person control and centralized media transfer center may not be practical at some sites (e.g., naval shipyards, naval vessels) because of physical site differences and the nature of work. When two-person control is not practical, mitigating circumstances and alternate protections should be determined by the cognizant DAA.

4) The following practical issues and mitigating circumstances should also be considered when developing two-person control methodologies:

a) Security enclosures around desktop computers may not be appropriate when the physical security of the site dictates the continued use of removable hard drives that are secured in safes when the computers are unattended (e.g., shift work).

b) The risk of unauthorized transfers may be lower when the majority of the workers on the site do not have and do not require access to most of the information on the classified network and adequate controls are in place to prevent their access.

c) Two-person control of information transfers may not be practical when production work is performed on off-shifts with limited staffing. However, a two-person review of the transfers could be conducted the next normal workday and periodic audits would determine the adequacy of the process and classification reviews.

d) Mitigation of the transfer risk should consider measures to minimize the amount of removable classified media produced and retained at a site. For example, electronic transfer over secure and accredited networks is preferred over generating media or shipping classified media.

e) Mitigation of the transfer risk must be addressed in system security plans.

i. Incident Response

A computer security incident response program is an essential component of the overall security measures that assist in protecting the information resources and data. Facilities processing classified or unclassified NNPI must have documented

incident response procedures that address discovery, reporting, evaluation and mitigation.

Incidents concerning NNPI on NMCI shall be handled in accordance with COMNAVNETWARCOM policy.

Some examples of incidents include (but are not limited to) the following:

- 1) Any act, intentional or unintentional, that violates a security policy.
- 2) Successful or failed attempts to gain unauthorized access to a system or its data.
- 3) Unexpected disruption or denial of service.
- 4) Unauthorized changes to system hardware, firmware or software characteristics without the system owner's knowledge, instruction or consent.
- 5) Unauthorized use of another user's account.
- 6) Unauthorized use of system privileges.
- 7) Intentional or unintentional execution of malicious code.

Other adverse events such as floods, fires, electrical outages, etc., that disrupt the operation of an information system falls outside the scope of this instruction and should be addressed in facility continuity of operations plans as required by the cognizant agency.

j. Wireless. Wireless devices, services, and technologies must comply with reference (g) or (q).

k. Training. Reference (a) requires computer security awareness training for all personnel who are involved with the management, use or operation of information systems processing sensitive US Government information. The requirements for the protection of NNPI on information systems shall be incorporated into local site training programs.

l. Approvals, Waivers and Exceptions.

Implementation of the computer security requirements identified in this instruction will be approved by the cognizant DAA. Waivers and exceptions to the requirements provided in

this document will be sent to NAVSEA 08Y for approval.
Implementation on old systems will be conducted to the extent
practical as determined by the cognizant DAA.

U-NNPI Information System Protection Requirements Checklist

This checklist must be completed to confirm compliance with the applicable security requirements. Each checklist shall also include a general description of applicable information systems/networks, and shall list the local cognizant security and management personnel responsible for the information systems/networks including those individuals authorized to make changes that would impact security.

SITE:	DATE PREPARED:
SITE ACRONYM:	

Description of Information Systems / Network	Responsible Local Security & Management Personnel (List Names, Titles, Phone Numbers)

Malicious Code	
All information systems/networks (workstations and servers) processing or storing U-NNPI must be configured with anti-viral software to actively monitor the system for viruses/malicious code and to perform periodic scanning of system hard drives. Virus definition files must be periodically updated. Controls must be in place to ensure that all files introduced onto the systems are scanned for viruses prior to use.	<input type="checkbox"/> (check if system complies)
Authentication and Identification	
The system requires a unique User ID and password for identification and authentication. User IDs and Passwords may be common/shared if the local DAA deems necessary to accomplish necessary tasks. Justification for allowing common/shared User IDs and Passwords must be included with the checklist.	<input type="checkbox"/>
Password aging, format and usage is in accordance with local policy.	<input type="checkbox"/>
Protections must be provided to preclude the compromise of passwords. Passwords shall be protected via appropriate access controls, by encryption, or both.	<input type="checkbox"/>
All default/initial system passwords are changed prior to production use.	<input type="checkbox"/>
Internet / Remote Access	
All modem and wireless access point connections are known, authorized, and properly secured.	<input type="checkbox"/>
All authorized transmissions of U-NNPI off-site, including access to U-NNPI by external dial-in systems, must be encrypted using a National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 compliant method as a minimum (hardware or software).	<input type="checkbox"/>

SITE:	DATE PREPARED:
SITE ACRONYM:	

The information system/network is utilizing a control interface equipment/solution (firewalls, IDS) to preclude unauthorized access from other information systems that are not authorized to process or store U-NNPI and from publicly accessible connections, such as the Internet. The local site will be responsible for managing this control interface equipment or has passed down the appropriate security requirements to a third party provider via contract.	<input type="checkbox"/>
Physical Protection	
Physical security controls are in place to prevent unauthorized physical access, tampering, damage and/or theft by an intruder with malicious intent of any sensitive IT resources (computer, servers, network devices, wiring closets).	<input type="checkbox"/>
Data Protection	
Access to U-NNPI data must be controlled based on need-to-know, ensuring that only authorized personnel may have access.	<input type="checkbox"/>
Protections must be provided to preclude unauthorized offloads/uploads. Authorized offloads/uploads must be conducted in accordance with local policy.	<input type="checkbox"/>
Media ingress/egress controls shall be in accordance with local policy.	<input type="checkbox"/>
Protections must be provided to preclude user account hijacking and masquerading. Local policy shall address acceptable control practices when the system with a logged-on user is unattended.	<input type="checkbox"/>
All output must be properly marked and secured in accordance with the applicable guidance.	<input type="checkbox"/>
User Acknowledgment	
All system users must review, agree to, and sign an Acceptable Use Policy that reflects the cognizant agency (DOD or DOE) requirements. The Acceptable Use Policy shall be made available for routine review by users.	<input type="checkbox"/>
A warning notice shall be displayed on all the information systems, conspicuously placed in close proximity to the system, or made available for routine review by users to warn users regarding inappropriate use of the system and to alert them that all actions on the system may be monitored.	<input type="checkbox"/>
Business Resumption	
Backups of data and configuration on the information systems/network and supporting equipment shall be performed in accordance with local policy. Identify whether a local back-up policy is in place.	<input type="checkbox"/>
Disaster recovery plans shall be established and implemented in accordance with local policy. Identify whether a disaster recovery plan is in place.	<input type="checkbox"/>



**REQUIREMENTS FOR VISITS TO NAVAL AND COMMERCIAL FACILITIES
PERFORMING NAVAL NUCLEAR PROPULSION WORK**

1. Visits to naval and commercial facilities performing naval nuclear propulsion work present unique security problems due to the need to protect both unclassified and classified NNPI from unauthorized access or release. In particular, the scope and complexity of the repair, overhaul and construction of U.S. Navy nuclear-powered ships is not always compatible with standard security and control measures. Access to NNPI is controlled principally by identifying and isolating areas within the facility which reveal NNPI. The security program necessary to protect NNPI will depend upon the type of work being performed and the personnel access control procedures in effect. In all cases, however, local activity or facility heads are responsible for establishing a security program which will ensure compliance with the disclosure policy of this instruction.

a. Visits by U.S. Citizens and U.S. Nationals. Reference (b) and the security provisions of applicable government contracts outline the required conditions, procedures, and responsibilities for visit approval.

b. Visits by Foreign Nationals or Representatives of a Foreign Interest

(1) References (b) and (e) and the security provisions of applicable government contracts apply. In addition, visits by foreign nationals or representatives of a foreign interest, whether for classified or unclassified purposes, require the specific approval of the NAVSEA (08) or designated representatives. Approval shall be obtained prior to the issuance of invitations or other commitments in order to protect NNPI and avoid unnecessary difficulties arising from denial of access. Requests for approval should contain activity plans for satisfying the special conditions outlined below. If all of these conditions cannot be satisfied, the visit shall either be diverted to an activity not engaged in naval nuclear propulsion work or be disapproved.

(a) The visitor(s) shall be kept under close and continuous surveillance at all times while within the physical confines of the facility.

(b) Visual, oral and documentary disclosures of NNPI shall be prevented by the isolation of areas, materials or personnel.

(c) The visit shall be accomplished without adverse impact on the facility's workload, scheduling or other critical management factors.

(2) The special considerations above for visits by a foreign national or representative of a foreign interest are not required for those personnel performing on a continuing basis custodial, maintenance, or administrative work that does not involve access to NNPI. In addition, in some instances foreign nationals or representatives of foreign interests may be able to gain access to or near facilities, specifically those which perform other diverse functions in addition to naval nuclear work, without being subject to formal access approval. In such cases, the activity is responsible for precluding, primarily through the isolation of areas or material which may reveal NNPI, and the control of personnel employed at the facility, unauthorized disclosure of NNPI.

(3) In accordance with the requirements of paragraph E3.1.3.1.2 of reference (e), foreign nationals or representatives of a foreign interest shall not be permitted access to the propulsion plant spaces of U.S. Navy nuclear-powered warships without the specific approval of the Chief of Naval Operations (CNO).

REQUIREMENTS FOR CONTRACTORS AND SUBCONTRACTORS

1. The requirements for the protection of NNPI are needed only in those contracts where there is a direct association with a naval nuclear propulsion plant application. When no such association exists, the contract does not involve access to NNPI and should not include contractual stipulations for its protection.
2. Activities which procure material, components or services involving access to NNPI shall ensure that appropriate requirements to control and protect NNPI are included in any such contracts or subcontracts.
3. When providing a specification, drawing or other technical document containing U-NNPI to a prospective contractor for purposes of soliciting bids where no contract yet exists, the contracting activity shall use a stipulation to obtain prospective contractor agreement to control or protect the U-NNPI until subsequent contractual controls are established. Attachment (1) is a sample stipulation.
4. Contracts or subcontracts involving classified NNPI must contain all required handling requirements for NNPI in the DD-254.
5. Contractors or subcontractors obligated under existing contracts to adhere to the guidelines of NN-801 (Guidelines for the Control and Protection of Unclassified Naval Nuclear Propulsion Information), NN-802 (Guidelines for the Control and Protection of Classified Naval Nuclear Propulsion Information), or NN-817 (Naval Nuclear Propulsion Information Guide), shall continue to utilize those guidelines for protection of NNPI.



**SAMPLE SECURITY AGREEMENT FOR PROTECTION OF UNCLASSIFIED NAVAL
NUCLEAR PROPULSION INFORMATION (U-NNPI)**

1. Purpose: The undersigned hereby agrees that when provided documents (specifications, drawings, etc.) that are marked as containing NOFORN sensitive information that must be controlled pursuant to federal law, the information contained therein and generated as part of the inquiry shall be used only for the purpose stated in the contract and shall in no case be transmitted outside the company (unless such transmittals comply with the detailed guidance of the contract) or to any foreign national within the company. While in use, the documents shall be protected from unauthorized observation and shall be kept secure so as to preclude access by any persons who do not have a legitimate need to view them. The documents shall not be copied unless done in conformance with the detailed guidance of the contract. All the documents shall be promptly returned in their entirety, unless authorized for proper disposal or retention, following completion of the contract.

2. Specific Requirements for Protecting U-NNPI:

(a) Only people who are a U.S. citizen and have a "Need to Know" required to execute the contract shall be allowed access to U-NNPI.

(b) When not in direct control of an authorized individual, U-NNPI must be secured in a locked container (e.g., file cabinet, desk, safe, etc.). Access to the container must be such that only authorized persons can access it and compromise of the container can be visually detected. Containers should have no labels that indicate the contents. If removed from the site, U-NNPI must remain in the personal possession of the individual. At no time should U-NNPI be left unsecured in a home or automobile, unattended in a motel room or sent with baggage, etc.

(c) Documents will have the word NOFORN at the top and bottom of each page. The cover sheet will have the warning statement shown below. Documents originated in the course of work that reproduce, expand or modify marked information shall be marked and controlled in the same way as the original. Media such as video tapes, disks, etc., must be marked and controlled similar to the markings on the original information.

NOFORN: This document is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with the prior approval of the Naval Sea Systems Command
--

(d) U-NNPI may not be processed on networked computers with outside access unless approved by the Naval Sea Systems Command. If desired the company may submit a proposal for processing NNPI on company computer systems. Personally owned computing systems, including, but not limited to, personal computers (PC), laptops, and Portable Electronic Devices (PED) such as Personal Digital Assistants (PDA), are not authorized for processing NNPI. Exceptions require the specific approval of the cognizant DAA and Naval Reactors (NR)/NAVSEA 08Y.

(e) U-NNPI may be faxed within the continental U.S. and Hawaii provided there is an authorized individual waiting to receive the document and properly control it. U-NNPI may not be faxed to facilities outside the continental U.S., including military installations, unless encrypted by Naval Sea System Command approved means.

(f) U-NNPI may be sent within the continental U.S. and Hawaii via first class mail in a single opaque envelope that has no markings indicating the nature of the contents.

(g) Disposal of documents containing U-NNPI shall ensure that the information is not easily retrievable. Disposing of documents in the same manner as classified documents is preferred.

(h) Report any attempts to elicit U-NNPI by unauthorized persons to the appropriate security personnel.

(i) Report any compromises of U-NNPI by unauthorized persons to the appropriate security personnel. This includes intentional or unintentional public release via such methods as theft, improper disposal (e.g., material not shredded, disks lost), placement on website, transmission via email, or violation of the information system containing U-NNPI.

Definitions applicable to this clause are provided in the base instruction.

EXHIBIT B

DEPARTMENT OF THE NAVY
Office of the Chief of Naval Operations
Washington, DC 20350-2000

OPNAVINST 5510.161
Op-009P3
Ser 09/5U301221
29 July 1985

OPNAV INSTRUCTION 5510.161

From: Chief of Naval Operations
To: All Ships and Stations

Subj: WITHHOLDING OF UNCLASSIFIED TECHNICAL DATA FROM PUBLIC DISCLOSURE

- Ref: (a) DOD Directive 5230.25 of 6 Nov 84 (NOTAL)
(b) Executive Order 12470 (NOTAL)
(c) Public Law 90-629, "Arms Export Control Act" as amended (22 U.S.C. Section 275 et seq.) (NOTAL)
(d) SECNAVINST 5720.42C
(e) OPNAVINST 5510.1G
(f) Militarily Critical Technologies List of Oct 84 (NOTAL)
(g) SECNAVINST 5720.44

- Encl: (1) Extract from the Export Administration Regulation (EAR)
(2) Extract from the International Traffic In Arms Regulation (ITAR)
(3) Definitions
(4) Sample Denial Letter for FOIA Requests
(5) Information Sheet on Qualified U.S. Contractors
(6) DD Form 2345
(7) Sample Denial Letter to Qualified U.S. Contractors - (Requests Unrelated to Certification)
(8) Notice to Accompany the Dissemination of Export Controlled Technical Data
(9) Sample Denial Letter to Qualified U.S. Contractors - (Requests Unrelated to DOD Support)
(10) Sample Denial Letter to persons not Qualified U.S. Contractors

1. Purpose. To implement reference (a) within the Department of the Navy (DON), to assign responsibilities, prescribe procedures and issue policy concerning the control of unclassified technical data by the DON.

2. Applicability and Scope. This instruction:

- a. Applies to all unclassified technical data that disclose critical technology with military or space application in

the possession of or under the control of the DON which may not be exported lawfully without an approval, authorization or license under references (b) or (c).

b. Does not introduce any additional controls on the dissemination of technical data by private enterprises or individuals beyond those specified by export control laws and regulations or in contracts or other mutual agreements, including certifications made pursuant to paragraph 4c. Accordingly, the mere fact that the DON may possess such data does not in itself provide a basis for control of these data pursuant to this instruction.

c. Does not introduce any controls on the dissemination of scientific, educational or other data that qualify for General License GTDA under export control law. Enclosures (1) and (2) are pertinent extracts from these laws; General License GTDA is defined in enclosure (1).

d. Does not alter the DON's responsibility to protect proprietary data of a private party in which the DON or the Department of Defense has "limited rights" or "restricted rights" (see enclosure (3), Definitions) or which are authorized to be withheld from public disclosure under the Freedom of Information Act, reference (d).

e. Does not pertain to or affect the release of technical data by the DON to foreign governments, international organizations or their respective representatives or contractors, pursuant to official agreements or formal arrangements with the U.S. Government or pursuant to U.S. Government-licensed transactions involving these entities or individuals.

f. Does not apply to classified technical data. After declassification, however, dissemination of such data that are within the scope of paragraph 2a is governed by this instruction. Reference (e) prescribes policy and procedures for the protection of classified information, including classified technical data.

3. Definitions. Terms used in this instruction are defined in enclosure (3).

4. Policy

- a. The DON may, pursuant to reference (a), withhold from public disclosure, notwithstanding any other provisions of law, any technical data that disclose critical



OPNAVINST 5510.161
29 July 1985

technology with military or space application in the possession of or under the control of the DON, if such data may not be exported lawfully without an approval, authorization or license under reference (c). Regulations issued under Executive Order or export control law (see enclosures (1) and (2)) may, in certain cases, authorize the export of technical data pursuant to a general unrestricted license or exemption. In these cases, the technical data covered by license or exemption may not be withheld.

b. Because public disclosure of technical data subject to this instruction is equivalent to providing uncontrolled foreign access, withholding these data from public disclosure, unless approved, authorized or licensed in accordance with export control law, is necessary and in the national interest. Unclassified technical data that are not governed by this instruction, unless otherwise restricted, shall continue to be made available to the public as well as to state and local governments.

c. Notwithstanding the authority provided in paragraph 4a, it is DON policy to provide technical data governed by this instruction to individuals and enterprises that are determined to be qualified U.S. contractors (see enclosure (3), Definitions), when the data are requested for a legitimate business purpose for which the contractor is certified by the Defense Logistics Services Center (DLSC), Battle Creek, Michigan. These certifications are valid for a period of 5 years. When the data are requested for a purpose other than to permit the requester to bid or perform on a contract with the DON, or other U.S. Government agency, and its release for purposes other than direct support of DON or other DOD activities may jeopardize an important U.S. technological or operational advantage, the data shall be withheld. Normally, this restriction will apply only in the case of Naval Nuclear Propulsion Information (NNPI) (as defined in reference (e)), polymer hydrophones/arrays related to submarine technology/design and to structural acoustic applications to submarine design. Commands desiring to have other classes of information included in this restriction against release may request approval from CNO (Op-009P). Requests must include a detailed justification and to be considered favorably, the technical data covered should provide a significant military capability and its development for commercial purposes would jeopardize the military advantage it provides. In the case of requests for large numbers of documents or extensive compilations of data which would tax a command's ability to reply in a timely fashion, the command concerned shall develop with the requester a mutually satisfactory delivery schedule. If

agreement cannot be reached, the matter shall be referred to CNO (Op-009P).

d. This instruction may not be used by DON commands as authority to deny access to technical data to the Congress, or to any Federal, State or local governmental agency that requires the data for regulatory or other official governmental purposes. Any such dissemination will include a statement that the technical data are controlled by the DON in accordance with this instruction.

e. The authority provided here may not be used to withhold from public disclosure unclassified information regarding DON operations, policies, activities or programs, including the costs and evaluations of performance and reliability of military and space equipment. When information of this kind contains technical data subject to this instruction, the technical data shall be excised prior to any public disclosure.

f. This instruction may not be used as a basis for the release of "limited rights" or "restricted rights" data as defined in enclosure (3), or that authorized to be withheld from public disclosure under the Freedom of Information Act (FOIA), implemented in the DON by reference (d).

g. This instruction may not be used to provide protection for technical data that should be classified in accordance with reference (e).

h. This instruction provides authority to cite "5 U.S.C. Section 552(b)(3)" (FOIA) as the basis for denials under the FOIA (see reference (d)) of technical data determined to be subject to the provisions of this instruction. See enclosure (4) for a sample denial letter for requests made under the FOIA.

5. Procedures

a. Requests for technical data shall be processed in accordance with chapter 12 of reference (e). FOIA requests for technical data subject to this instruction shall be handled in accordance with reference (d). FOIA requests for technical data determined to be subject to the withholding authority effected by this instruction shall be denied under 5 U.S.C. Section 552(b)(3), and the requester shall be referred to the provisions of this instruction permitting access by qualified U.S. contractors. Enclosure (4) is a sample denial letter for requests for unclassified technical data under the FOIA. Enclosure (5) is a sample information sheet pertaining to qualified U.S. contractors which shall be furnished each requester with letters of denial.

b. Upon receipt of a request for technical data in the possession of or under the control of the DON, the controlling Navy or Marine Corps command (see enclosure (3), Definitions) shall determine whether the data are governed by this instruction. This determination shall be based on the following:

(1) The command's findings that the data would require an approval, authorization or license for export under references (b) or (c), and that the data may not be exported pursuant to a general, unrestricted license (see enclosure (1)) or exemption (see enclosure (2)). Commands may, in cases where such determinations cannot readily be made locally, request guidance on specific cases from CNO (Op-009P). It is not intended, however, that all requests be referred routinely to CNO for decision.

(2) The command's judgment that the technical data under consideration disclose critical technology with military or space application. For purposes of making these determinations, the Militarily Critical Technologies List (MCTL), reference (f), shall be used as general guidance. The controlling DON command may request assistance in making these determinations from the Office of the Under Secretary of Defense for Research and Engineering (OUSDR&E) via CNO (Op-009P).

c. Requests from foreign governments, organizations or individuals for technical data shall be referred to CNO (Op-62).

d. The controlling command shall ensure that technical data determined to be governed by this instruction are marked in accordance with chapter 12 of reference (e). All technical documents determined to be subject to the withholding provisions of this instruction will be marked with an export warning notice as follows: "WARNING. This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. Section 2751 et seq.) or Executive Order 12470. Violations of these export laws are subject to severe criminal penalties."

e. A controlling command shall release technical data governed by this instruction only to a qualified U.S. contractor, as evidenced by the contractor's submission of a completed DD 2345, enclosure (6), with each request for unclassified technical data subject to this instruction. The certification process has been established to assist the controlling Navy or Marine Corps command (see enclosure (3), Definitions) in determining as efficiently as possible whether the requester should receive the technical

data requested. A certified requester is not automatically qualified to receive all DON export controlled information. The controlling command must ensure that the "qualified contractor" is qualified to receive the particular type of information requested. Command release authority may be exercised unless one of the following apply:

(1) The qualification of the U.S. contractor concerned has been revoked temporarily in accordance with paragraph 5i; or

(2) The requested data are judged to be unrelated to the purpose for which the qualified U.S. contractor is certified. When release of technical data is denied in accordance with this paragraph, the controlling command shall inform the U.S. contractor of the reasons for the denial, i.e., the requested data are deemed to be unrelated to the U.S. contractor's certification. The letter of denial, enclosure (7), is a sample of such a letter and shall advise the U.S. contractor that application can be made to the DLSC for a new certification and request additional information which would describe intended use of the requested data; or

(3) The technical data are being requested for a purpose other than to permit the requester to bid or perform on a contract with the DON or other U.S. Government agency. In these cases, the controlling command shall withhold the data if it has been determined by the originating command (see enclosure (3), Definitions) that the significance of the data for military purposes precludes its release for purposes other than direct support of DON approved activities, because release could jeopardize an important technical or operational military advantage of the United States (normally applicable only to NNPI, polymer hydrophones/arrays and structural acoustic applications to submarine design); or

(4) There is reason to question the validity of the U.S. contractor's qualification, in which case the Chief of Naval Operations (Op-009P) is to be notified immediately. Reasons for casting doubt upon the validity of a U.S. contractor's qualification could be, but are not limited to, a certification date of more than 5 years from date of issue; an apparent alteration of the submitted DD 2345; the use of type faces, numbers, titles or other detail which appear different from those previously observed on other DD 2345; or the use of foreign addresses or firms as proposed recipients of controlled data.

f. Any release to qualified U.S. contractors of technical data controlled by this instruction shall be accompanied by

29 July 1985

a notice to the recipient as set forth in enclosure (8). Documents being mailed to a qualified U.S. contractor shall be sent to the address shown for the data recipient in block 3 of the DD 2345 regardless of any request for mailing to a different address. Commands shall deny requests from qualified U.S. contractors that specify the data be sent to an address outside the United States.

g. Commands will deny all non-FOIA requests for unclassified technical data covered by this instruction which are not accompanied by a completed DD Form 2345. Commands may confirm, when necessary, a requester's qualification as a U.S. contractor by:

(1) Contacting the DLSC at Autovon 369-9288/89 or FTS 372-9288/89 or commercial (616) 962-6511, extension 9288, to ensure that the requester is listed by the DLSC as a qualified U.S. contractor; and

(2) Reviewing the listing published by CNO (Op-009P) of revocations and suspensions of U.S. contractors' qualifications to ensure that requesters have not been debarred from receiving such data.

h. If a request is denied because of use of an invalid DD 2345, the matter shall be reported immediately to CNO (Op-009P). Reports will contain, as a minimum, the date of the request, the name and affiliation of the requester, a copy of the DD 2345 and an explanation as to why the form was deemed to be invalid.

i. Commands becoming aware of credible and sufficient information that a qualified U.S. contractor has (1) violated U.S. export control law, (2) violated its certification, (3) made an application for certification in bad faith or (4) made an omission or misstatement of material fact will report this information to CNO (Op-009P). CNO (Op-009P) will, in coordination with the General Counsel of the Navy and the Judge Advocate General of the Navy, revoke temporarily the U.S. contractor's qualification. Revocations having the potential for compromising a U.S. Government investigation may be delayed. Immediately upon a contractor's revocation, CNO (Op-009P) shall notify the contractor, the OUSDR&E and all DON commands on distribution for receipt of contractor qualification revocations or suspensions. The contractor concerned shall be given an opportunity to respond in writing to the information upon which the temporary revocation is based before being disqualified. Any U.S. contractor whose qualification has been revoked temporarily may be reinstated by CNO (Op-009P) upon presentation of sufficient informa-

tion showing that the basis for the revocation was in error or has been remedied.

j. When the basis for a contractor's temporary revocation cannot be removed within 20 working days, CNO (Op-009P) shall recommend to the OUSDR&E that the contractor be disqualified.

k. Charges for copying, certifying and searching records provided to requesters shall be levied in accordance with charges authorized by the NAVCOMPT Manual, paragraph 035887. Normally, only one copy of the same record or document will be provided to each requester.

l. Technical documents marked with distribution limitation statements (see Exhibit 12B of reference (e)) which require originator approval prior to release may not be released without such approval. In these cases, a requester may be advised that his request requires originator approval and that the approval has been requested. In these cases controlling commands will request the approval of the originating command prior to release of the requested information. Originating commands shall approve release of their controlled information if assured by the controlling command that the requester is a qualified U.S. contractor, unless the request should be denied for the reasons permitted in paragraph 5e. Unclassified technical data pertaining to naval nuclear propulsion matters requires CNO (OP-00N) approval prior to its release by any controlling command. Unclassified technical data pertaining to submarine matters or operations requires CNO (Op-02) approval prior to its release by any controlling command. Requests for technical data requiring release approval by other DOD or Government agencies shall be referred to those agencies.

m. Unless advised to the contrary, qualified U.S. contractors who receive technical data governed by this instruction may disseminate the data for purposes consistent with their certifications without the prior permission of the controlling Navy command. Qualified U.S. contractors may also disseminate such data without prior permission to:

(1) Any foreign recipient for which the data are approved, authorized or licensed under references (b) or (c);

(2) Another qualified U.S. contractor, as defined in enclosure (3), including existing or potential subcontractors, but only within the scope of the certified legitimate business purpose of the recipient;

(3) The Departments of State and Commerce, for purposes of applying for appropriate approvals, authorizations or licenses for export under references (b) or (c). Any such application shall include a statement that the technical data for which approval, authorization or license is sought are controlled by the Department of the Navy in accordance with this instruction;

(4) Congress or to any Federal, State or local governmental agency for regulatory purposes, or otherwise as may be required by law or court order. Disseminations shall include a statement that the technical data are controlled by the DON in accordance with this instruction.

n. A qualified U.S. contractor desiring to disseminate technical data subject to this instruction in a manner not permitted expressly by the terms of this instruction shall seek authority to do so from the controlling DON command. A command receiving such request from a qualified U.S. contractor shall refer the request to the command or office which originated the information. If the originator cannot be ascertained, the request shall be referred to CNO (Op-009P). Unauthorized redissemination of technical data subject to this instruction by a qualified U.S. contractor can take place by the publishing of articles in open literature, in advertising or in promotional materials, in conducting educational and training courses, and by similar means where persons or entities not authorized by this instruction to have access to the technical data can obtain access.

o. Any requester denied technical data or any qualified U.S. contractor denied permission to re-disseminate technical data pursuant to this instruction shall be provided a written statement of reasons for that action within 15 days of such denial and advised of the right to make a written appeal to CNO (Op-009P). Appeals of denials made under FOIA shall be handled in accordance with procedures established by reference (d). Other appeals shall be processed as directed by CNO (Op-009P). Enclosure (9) is a sample letter of denial to qualified U.S. contractors. Enclosure (10) is a sample denial letter used for denials to requesters who are not qualified U.S. contractors.

p. Denials for other than FOIA requests shall cite "10 U.S.C. Section 140c as implemented by DOD Directive 5230.25 of 6 Nov 1984" (NOTAL). FOIA denials shall cite "5 U.S.C. Section 552(b)(3)," reference (d). Denial letters shall be modelled after the formats set out in enclosures (4), (7), (9) and (10).

q. Requests for technical data from foreign individuals or entities shall be forwarded to CNO (Op-62).

r. When disclosure of export-controlled technical data is necessary to a procurement, the command concerned must ensure that all who receive the data are qualified U.S. contractors. Information for Bids and Requests for Proposals may include notification that only contractors certified under DOD procedures, reference (a), may receive export-controlled technical data from the DON. Such notification, if used, shall include information about the qualified U.S. contractor program, enclosure (5).

6. Responsibilities

a. Under the Chief of Naval Operations:

(1) The Director, Security Policy Division (Op-009P) is responsible for the implementation of this instruction and shall:

(a) Administer and monitor compliance with this instruction.

(b) Receive and disseminate notifications of temporary revocation in accordance with paragraph 5i.

(c) Receive recommendations from DON commands for contractor disqualification and notify the OUSDR&E pursuant to paragraph 5i.

(d) In coordination with the OASNRE&S and the Director, Research Development, Test and Evaluation (Op-098), issue guidance which identifies the technical data subject to this instruction.

(2) The Director, Technology Transfer Policy and Control Division (Op-62) is responsible for the release of technical data covered by this instruction to foreign persons or entities, except for that data covered in subparagraph 5m(1).

b. Commanding officers are responsible for ensuring that technical data subject to this instruction in their possession or under their control are handled in accordance with this instruction.

c. Persons in the naval establishment who have or have had access to technical data covered by this instruction are responsible for the safeguarding and control of

OPNAVINST 5510.161

29 July 1985

the data in accordance with this instruction. Naval personnel, military and civilian, may not publicly disclose such data without formal command approval. See reference (g).

d. The Judge Advocate General and the General Counsel, as appropriate, are responsible for ensuring the procedural sufficiency and substantive lawfulness of U.S. contractor certification revocations. The General Counsel is responsible for providing legal review of FOIA request denials when requested.

7. Report. The report required by paragraph 5 is assigned report control symbol OPNAV 5510-23 and is approved for 3 years only from the date of this directive.

8. Form. DD 2345 (Rev Dec 85), S/N 0102-LF-002-3450, may be obtained through normal Navy supply channels in accordance with NAVSUP P-2002.

RONALD J. HAYS
Vice Chief of Naval Operations

Distribution:
SNDL Parts 1 and 2
MARCORPS Code DS

Commander
Naval Data Automation Command (Code 172)
Washington Navy Yard
Washington, D.C. 20374-1662 (200 copies)

Stocked:
CO, NAVPUBFORMCEN
5801 Tabor Avenue
Philadelphia, PA 19120-5099 (500 copies)