Under Article 1904 of the Agreement, which came into force on January 1, 1994, the Government of the United States, the Government of Canada and the Government of Mexico established *Rules of Procedure for Article 1904 Binational Panel Reviews* (''Rules''). These Rules were published in the **Federal Register** on February 23, 1994 (59 FR 8686). The panel review in this matter was requested and terminated pursuant to these Rules.

Dated: May 30, 2002.

Caratina L. Alston,

United States Secretary, NAFTA Secretariat.

[FR Doc. 02–15323 Filed 6–17–02; 8:45 am]

BILLING CODE 3510–GT–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 020503109–2109–01]

RIN 0693–AB51

Establishment of Information Technology Security Validation Programs Fees

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) operates a number of Information Technology Security Validation Programs. Under these programs, vendors use independent private sector, accredited testing laboratories to have their products tested. The goal of the Information Technology Security Validation Programs is to promote the use of validated products and provide Federal agencies and other users with a security metric to use in procuring software and equipment. The results of the independent testing performed by accredited laboratories provide this metric. NIST validates the test results and issues validation certificates. NIST also posts and maintains the validated products lists on the Computer Security Division Web site. The Information Technology Security Validation Programs currently do not charge a fee for their services, but demand for these services as increased over 1800% since 1996 in some cases. This growth has resulted in significantly increased expense to NIST for program management and associated functions. NIST issues this notice to adopt a fee schedule for some of the Information Technology Security Validation Programs, with fees being set individually for each program. The fees will allow NIST to continue and expand the Information Technology Security Validation Programs.

DATES: This notice is effective July 18, 2002.

FOR FURTHER INFORMATION CONTACT: Ray Snouffer, Computer Security Division, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899–8930, telephone (301) 975–4436, e-mail: *ray.snouffer@nist.gov.*

SUPPLEMENTARY INFORMATION: Federal agencies, industry, and the public now rely on a number of measures for the protection of information and communications used in electronic commerce, critical infrastructure and other application areas. Though these measures are used to provide security, weaknesses such as poor design can render the product insecure and place highly sensitive information at risk. Adequate testing and validation against established standards is essential to provide security assurance. NIST operates a number of established Information Technology Security Validation Programs. Under these programs, vendors use independent private sector, accredited testing laboratories to have their products tested. The goal of the Information Technology Security Validation Programs is to promote the use of validated products and provide Federal agencies and other users with a security metric to use in procuring software and equipment. The results of the independent testing performed by accredited laboratories provide this metric. Federal agencies, industry, and the public can choose products from the Validated Products List and have increased confidence that the products meet their claimed levels of performance and security.

NIST validates the test results and issues validation certificates. NIST also posts and maintains the validated products lists on the Computer Security Division web site. Since the IT standards, security specifications, and NIST security recommendations, which underlie the testing programs must be flexible enough to adapt to advancements and innovations in science and technology, NIST continually performs reviews and updates. This process is based on technological and economical changes, which require research and interpretation of the standards.

The Information Technology Security Validation Programs currently do not charge a fee for their services, but demand for these services as increased over 1800% since 1996 in some cases. This growth has resulted in significantly increased expense to NIST for program management and associated functions. NIST proposes to adopt a fee schedule for some of the Information Technology Security Validation Programs with fees being set individually for each program. The fees will allow NIST to continue and expand the Information Technology Security Validation Programs. Fees will be subjected to an annual cost-analysis to determine if the fees need adjustment.

The first Information Technology Security Validation Program to charge a fee will be the Cryptographic Module Validation Program (CMVP). Each of the Rating Levels (1–4) will have a different fee. Every Validation report will be charged a ''baseline'' fee. Baseline fees will accompany each validation report submitted to NIST. Validation reports will not be reviewed until such time as NIST receives payment of the baseline fee from the vendor. Validation reports that necessitate extended evaluation and collaboration with the certifying laboratory will be charged an additional ''extended'' fee. The baseline and extended fees for each Rating Level will be:

Level	Baseline fee	Extended fee	Total possible fee
1	$2750	$1250	$4000
2	3750	1750	5500
3	5250	2500	7750
4	7250	3500	10750

All fees are given in US dollars.

The levels specified above are commensurate with the security testing levels applied by the Cryptographic Module Testing laboratories in determining compliance with FIPS 140–2. A government and industry working group composed of both users and vendors developed FIPS 140–2. The working group identified eleven areas of security requirements with four increasing levels of security for cryptographic modules. The security levels allow for a wide spectrum of data sensitivity (*e.g.,* low value administrative data, million dollar funds transfers, and health data), and a diversity of application environments (*e.g.,* a guarded facility, an office, and a completely unprotected location). Each security level offers an increase in security over the preceding level.

Authority: NIST's activities to protect Federal sensitive (unclassified) systems are undertaken pursuant to specific responsibilities assigned to NIST in section 5131 of the Information Technology

Management Reform Act of 1996 (Pub. L. 104–106), the Computer Security Act of 1987 (Pub. L. 100–235), and Appendix III to Office of Management and Budget Circular A–130. NIST's authority to perform work for others and charge fees for those services is found at 15 U.S.C. 273 and 275a.

Classification: Because notice and comment are not required under 5 U.S.C. 553 or any other law, for matters relating to agency management or personnel or to public property, loans, grants, benefits, or contracts, a regulatory flexibility analysis (5 U.S.C. 601 *et seq.*) is not required and has not been prepared.

Executive Order 12866: This notice has been determined to be not significant for the purposes of Executive Order 12866.

Dated: June 12, 2002.

Karen H. Brown,

Deputy Director.

[FR Doc. 02–15278 Filed 6–17–02; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Availability of Seats for the Olympic Coast National Marine Sanctuary Advisory Council

AGENCY: National Marine Sanctuary Program (NMSP), National Ocean Service (NOS), National Oceanic and Atmospheric Administration, Department of Commerce (DOC).

ACTION: Notice and request for applications.

SUMMARY: The Olympic Coast National Marine Sanctuary (OCNMS or Sanctuary) is seeking applicants for the following vacant seat on its Sanctuary Advisory Council (Council): alternate for Tourism/Recreation. Applicants are chosen based upon their particular expertise and experience in relation to the seat for which they are applying; community and professional affiliations; philosophy regarding the conservation and management of marine resources; and possibly the length of residence in the area affected by the Sanctuary. The selected alternate will serve a term that expires at the end of the current member's term.

DATES: Applications are due by July 12, 2002.

ADDRESSES: Application kits may be obtained from Andrew Palmer, OCNMS, 138 West First St., Port Angeles, WA 98362 Completed applications should be sent to the same address.

FOR FURTHER INFORMATION CONTACT: Andrew Palmer at (360) 457–6622 x30 or *andrew.palmer@noaa.gov.*

SUPPLEMENTARY INFORMATION: The Sanctuary Advisory Council provides NOAA with advice on the management of the Sanctuary. Members provide advice to the Olympic Coast Sanctuary Superintendent on Sanctuary issues. The Council, through its members, also serves as liaison to the community regarding Sanctuary issues and acts as a conduit, relaying the community's interests, concerns, and management needs to the Sanctuary.

The Sanctuary Advisory Council members represent public interest groups, local industry, commercial and recreational user groups, academia, conservation groups, government agencies, and the general public.

Authority: 16 U.S.C. Section 1431 et seq.

(Federal Domestic Assistance Catalog Number 11.429 Marine Sanctuary Program)

Dated: June 10, 2002.

Jamison S. Hawkins,

Deputy Assistant Administrator for Ocean Services and Coastal Zone Management.

[FR Doc. 02–15288 Filed 6–17–02; 8:45 am]

BILLING CODE 3510–08–M

DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Representative and Address Provisions

ACTION: Proposed collection; comment request.

SUMMARY: The United States Patent and Trademark Office (USPTO), as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on the revision of a continuing information collection, as required by the Paperwork Reduction Act of 1995, Public Law 104–13 (44 U.S.C. 3506(c)(2)(A)).

DATES: Written comments must be submitted on or before August 19, 2002.

ADDRESSES: Direct all written comments to Susan K. Brown, Records Officer, Office of Data Management, Data Administration Division, USPTO, Suite 310, 2231 Crystal Drive, Washington, DC 20231; by telephone at (703) 308–7400; or by electronic mail at *susan.brown@uspto.gov.*

FOR FURTHER INFORMATION CONTACT: Requests for additional information should be directed to Robert J. Spar, Director, Office of Patent Legal Administration, USPTO, Washington, DC 20231; by telephone at (703) 308–5107; or by electronic mail at *bob.spar@uspto.gov.*

SUPPLEMENTARY INFORMATION:

I. Abstract

Under 35 U.S.C. 2 and 37 CFR 1.31–1.36 and 1.363, a patent applicant or assignee of record may grant power of attorney or authorization of agent to a person who is registered to practice before the United States Patent and Trademark Office (USPTO) to act for them in a representative capacity on a patent or application. A power of attorney or authorization of agent may also be revoked, and a registered representative may also withdraw as attorney or agent of record under 37 CFR 1.36. The rules of practice (37 CFR 1.33) also provide for the applicant, patentee, assignee, or representative of record to supply a correspondence address and daytime telephone number for receiving notices, official letters, and other communications from the USPTO. Further, the rules of practice (37 CFR 1.33(d) and 1.363) permit the applicant, patentee, assignee, or representative of record to specify a separate ''fee address'' for correspondence related to maintenance fees, which is covered under OMB Control Number 0651–0016 ''Rules for Patent Maintenance Fees.'' Maintaining a correct and updated correspondence address is necessary so that correspondence from the USPTO related to a patent or application will be properly received by the applicant, patentee, assignee, or authorized representative.

The USPTO's Customer Number practice permits applicants, patentees, assignees, and registered representatives to efficiently change the correspondence address or registered representatives for a number of patents or applications with one change request instead of filing separate change requests for each patent or application. Customers may request a customer number from the USPTO and associate this customer number with a correspondence address or a list of registered practitioners. Customers may then use this customer number to designate or change the correspondence address or to grant power of attorney to the list of registered practitioners for any number of patents or applications. Any changes to the address or practitioner information associated with a customer number will be applied to all patents and applications associated with that customer number.

The Customer Number practice is optional, in that changes of