FOR FURTHER INFORMATION CONTACT: Zev Primor or Maisha Cryor, AD/CVD Enforcement, Group II, Office 4, Import Administration, International Trade Administration, U.S. Department of Commerce, 14th Street and Constitution Avenue, NW, Washington, DC 20230; telephone (202) 482–4114 or (202) 482–5831, respectively.

SUPPLEMENTARY INFORMATION:

Background

On July 3, 2003, Tyco requested that the Department conduct an expedited changed circumstances review of the antidumping duty order on PSPT from Italy pursuant to section 751(b)(1) of the Act and 19 CFR 351.221(c)(3)(ii). Tyco claims to be the successor-in-interest to Manuli Autoadesivi (Manuli), based on its May 8, 2001, purchase of Manuli Tapes[1], and, as such, claims that it is entitled to receive the same antidumping treatment as Manuli.

Scope of Review

Imports covered by the review are shipments of PSPT measuring 1 3/8 inches in width and not exceeding 4 millimeters in thickness, currently classifiable under items 3919.90.20 and 3919.90.50 of the Harmonized Tariff Schedule of the United States (HTSUS). HTSUS subheadings are provided for convenience and customs purposes. The written description remains dispositive as to the scope of the product coverage.

Initiation of Antidumping Duty Changed Circumstances Review

Pursuant to section 751(b)(1) of the Act, the Department will conduct a changed circumstances review upon receipt of information concerning, or a request from an interested party for a review of, an antidumping duty order which shows changed circumstances sufficient to warrant a review of the order. The information submitted by Tyco regarding a change in ownership of Manuli shows changed circumstances sufficient to warrant a review. *See* 19 CFR 351.216(c) (2003).

In antidumping duty changed circumstances reviews involving a successor-in-interest determination, the Department typically examines several factors including, but not limited to, changes in: (1) management; (2) production facilities; (3) supplier relationships; and (4) customer base. *See Brass Sheet and Strip from Canada: Notice of Final Results of Antidumping Administrative Review*, 57 FR 20460, 20462 (May 13, 1992) (*Canadian Brass*). While no single factor or combination of factors will necessarily be dispositive, the Department generally will consider the new company to be the successor to the predecessor company if the resulting operations are essentially the same as those of the predecessor company. *See, e.g., Industrial Phosphoric Acid from Israel: Final Results of Changed Circumstances Review*, 59 FR 6944, 6945 (February 14, 1994), and *Canadian Brass*, 57 FR 20460. Thus, if the record evidence demonstrates that, with respect to the production and sale of the subject merchandise, the new company operates as the same business entity as the predecessor company, the Department may assign the new company the cash deposit rate of its predecessor. *See, e.g., Fresh and Chilled Atlantic Salmon from Norway: Final Results of Changes Circumstances Antidumping Duty Administrative Review*, 64 FR 9979, 9980 (March 1, 1999). Although Tyco submitted information indicating, allegedly, that, with respect to subject merchandise, it operates in the same manner as its predecessor, that information is unclear and is lacking sufficient supporting documents. *See* Letter from the Department to Tyco, Re: ''Pressure Sensitive Plastic Tape from Italy: Changed Circumstances Review, Supplemental Questionnaire'' dated July 10, 2003. Concerning Tyco's request that the Department conduct an expedited antidumping duty changed circumstances review, the Department has determined that it would be inappropriate to expedite this action by combining the preliminary results of review with this notice of initiation, as permitted under 19 CFR 351.221(c)(3)(ii). Because the Department may need to seek additional information, we find that an expedited action is impracticable. Therefore, the Department is not issuing the preliminary results of its antidumping duty changed circumstances review at this time.

The Department will publish in the **Federal Register** a notice of preliminary results of antidumping duty changed circumstances review, in accordance with 19 CFR 351.221(b)(4) and 19 CFR 351.221(c)(3)(I). This notice will set forth the factual and legal conclusions upon which our preliminary results are based and a description of any action proposed based on those results. Pursuant to 19 CFR 351.221(b)(4)(ii), interested parties will have an opportunity to comment on the preliminary results of review. In accordance with 19 CFR 351.216(e), the Department will issue the final results of its antidumping duty changed circumstances review not later than 270 days after the date on which the review is initiated.

During the course of this antidumping duty changed circumstances review, we will not change the cash deposit requirements for the merchandise subject to review. The cash deposit will only be altered, if warranted, pursuant to the final results of this review. This notice of initiation is in accordance with sections 751(b)(1) of the Act and 19 CFR 351.221(b)(1) of the Department's regulations.

Dated: August 18, 2003.

Jeffrey May,

Acting Assistant Secretary for Import Administration.

[FR Doc. 03–21842 Filed 8–26–03; 8:45 am]

BILLING CODE 3510–DS–S

[1] On December 31, 1999, after merging with another company, Manuli changed its corporate name to Manuli Tapes S.p.A.

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 030711167–3167–01]

Notice of Request for Submissions of Information Security Practices by Public and Private Sector Organizations

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice.

SUMMARY: NIST invites public and private organizations to submit their information security practices for inclusion in its Computer Security Resource Center. The NIST Computer Security Resource Center (CSRC) Web site, located at *http://csrc.nist.gov*, houses security specific guidance and tools that are shared widely in support of improving security programs and fostering good security practice. Selected information security practices will be posted on the Federal Agency Security Practices (FASP) section of the CSRC Web page (*http://csrc.nist.gov/fasp*). FASP includes a variety of agency security practices, which have been successfully used by the submitters in implementing their information security programs. With the recognition that protection of the Nation's critical infrastructure is dependent upon effective information security solutions and to minimize vulnerabilities associated with a variety of threats, the broader sharing of such practices will enhance the overall security of the nation. Today's federal networks and systems are highly interconnected and interdependent with non-federal systems. Access to information security

practices in the public and private sector can be applied to enhance the overall performance of Federal information security programs.

DATES: Request period is open-ended. Submissions can be offered at any time.

ADDRESSES: Written submissions may be sent to Computer Security Division, ATTN: Information Security Practices, Mail Stop 8930, 100 Bureau Drive, Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930. Electronic submissions should be sent to: *infosecpractices@nist.gov.* Materials accepted by NIST will be posted to its CSRC Web site at *http://csrc.nist.gov/pcig.*

FOR FURTHER INFORMATION CONTACT: Ms. Joan Hash, (301) 975–3357, National Institute of Standards and Technology, Attn: Computer Security Division, 100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899–8930, e-mail: *joan.hash@nist.gov.*

SUPPLEMENTARY INFORMATION: Under section 5131 of the Information Technology Management Reform Act of 1996 and sections 302–3 of the Federal Information Security Management Act of 2002 (FISMA) (Pub. L. 107–347), the Secretary of Commerce is authorized to approve standards and guidelines for Federal information systems and to make standards compulsory and binding for Federal agencies as necessary to improve the efficiency or security of Federal information systems. NIST is authorized to develop standards, guidelines, and associated methods and techniques for information systems, other than national security systems, to provide for adequate information security for agency operations and assets. The FISMA requires each Federal agency to develop, document, and implement an agency-wide information security program that will provide information security for the information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The FISMA specifically tasked NIST to evaluate public and private sector security practices. This is done to improve the level of Federal security programs and to learn from public and private sector best practices.

NIST invites public and private organizations to submit their information security practices for inclusion in its Computer Security Resource Center. The NIST CSRC Web site, located at *http://csrc.nist.gov* specific guidance and tools that are shared widely in support of improving security programs and fostering good security practice. Selected information security practices will be posted on the FASP section of the CSRC Web page (*http://csrc.nist.gov/fasp*). FASP includes a variety of agency security practices, which have been successfully used by the submitters in implementing their information security programs. With the recognition that protection of the Nation's critical infrastructure is dependent upon effective information security solutions and to minimize vulnerabilities associated with a variety of threats, the broader sharing of such practices will enhance the overall security of the nation. Today's Federal networks and systems are highly interconnected and interdependent with non-Federal systems. Access to information security practices in the public and private sector can be applied to enhance the overall performance of Federal information security programs.

Submitters must indicate the source of the information security practices, such as an official organization Web site, or they may submit their information security practices accompanied by a management official's approval. Submitters may request that NIST sanitize the submission to mask the source of the material. NIST will review submissions for consistency with generally accepted security practices prior to posting. These practices may be found at *http://csrc.nist.gov/publications/*. Submissions must include a point of contact. NIST reserves the right to accept, post and remove submissions at its discretion. By submitting material, the submitter agrees that NIST may publicly disseminate such material, regardless of copyright. Submitters agree to inform NIST if the status of the submission changes (updated, discontinued, etc.). The preferred method of transmittal of the submissions is via e-mail to *infosecpractices@nist.gov.*

Policies and procedures may be submitted to NIST in any area of information security including, but not limited to: Accreditation, audit trails, authorization of processing, budget planning and justification, certification, contingency planning, data integrity, disaster planning, documentation, hardware and system maintenance, identification and authentication, incident handling and response, life cycle, network security, personnel security, physical and environmental protection, production input/output controls, security policy, program management, review of security controls, risk management, security awareness training, and education (to include specific course and awareness materials), and security planning.

Dated: August 21, 2003.

Hratch G. Semerjian,

Acting Deputy Director.

[FR Doc. 03–21948 Filed 8–26–03; 8:45 am]

BILLING CODE 3510–CN–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcing a Meeting of the Information Security and Privacy Advisory Board

AGENCY: National Institute of Standards and Technology.

ACTION: Notice of meeting.

SUMMARY: Pursuant to the Federal Advisory Committee Act, 5 U.S.C. App., notice is hereby given that the Information Security and Privacy Advisory Board (ISPAB) will meet Tuesday, September 16, 2003, from 8:30 a.m. until 5 p.m., Wednesday, September 17, 2003, from 8:30 a.m. until 5 p.m. and on Thursday, September 18, from 8:30 a.m. until 1 p.m. All sessions will be open to the public. The Advisory Board was established by the Computer Security Act of 1987 (Pub. L. 100–235) and amended by the Federal Information Security Management Act of 2002 (Pub. L. 107–347) to advise the Secretary of Commerce and the Director of NIST on security and privacy issues pertaining to federal computer systems. Details regarding the Board's activities are available at *http://csrc.nist.gov/ispab/*.

DATES: The meeting will be held on September 16, 2003, from 8:30 a.m. until 5 p.m., September 17, 2003, from 8:30 a.m. until 5 p.m., and September 18, 2003, from 8:30 a.m. until 1 p.m.

ADDRESSES: The meeting will take place at the Bethesda Hyatt Regency Hotel, 7400 Wisconsin Avenue [One Bethesda Metro Center], Bethesda, MD 20814.

Agenda

—Welcome and Overview
—Session on Agencies Customer Service Management Work
—Session on the National Information Assurance Program Extension Activities
—Session on Acceptable Behavior of ''Touching the Browser''
—NIST Information Technology Laboratory Briefings
—Update by OMB on Privacy and Security Issues
—Briefing by Department of Homeland Security Office Privacy Officer