

minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government." Various Federal organizations (NIST, NSA, DISA, etc.), consortia (e.g., Center for Internet Security), and some commercial vendors produce these checklists. Such checklists when combined with well-developed guidance, leveraged with high-quality security expertise, vendor product knowledge, operational experience, and accompanied with tools can markedly reduce the vulnerability exposure of an organization. To meet this challenging requirement to produce checklists for the spectrum of IT products widely used in the government, NIST has developed a proposal to solicit from IT vendors, consortia, industry and government organizations, and others in the public and private sector to produce additional checklists and associated guidance material to NIST. These materials would then be made available for display and downloading from the NIST Computer Security Resource Center (CSRC) Web site (<http://csrc.nist.gov>). To gather feedback on the proposed approach, NIST is announcing a workshop to identify current and planned Federal government checklist activities and related needs, existing and planned voluntary efforts for building security checklists, and current industry capabilities for the development of checklists and the associated templates that describe sets of security configurations for IT products widely used in the United States Government (USG).

It is anticipated that the workshop will support the development of a standard Extensible Markup Language (XML) template for security configuration checklist descriptions, and a guideline on producing consensus checklists that can be searched, compared, shared freely, and used by the USG and Internet community at large. The goal of this initial workshop is to collect suggestions from organizations that have already developed or are involved in the development of such checklists to gain their input on key items that should be included within the template. The detailed draft agenda and supporting documentation for the workshop will be available prior to the workshop from the NIST CSRC Web site at <http://csrc.nist.gov/checklists> by July 31, 2003.

DATES: The workshop will be held on September 25 and 26, 2003, from 9 a.m. to 5 p.m.

ADDRESSES: The workshop will be held in the Lecture Room B, Bldg 101 at the National Institute of Standards and Technology, Gaithersburg, MD.

FOR FURTHER INFORMATION CONTACT: Additional information, when available, may be obtained from the Computer Security Resource Center Web site at <http://csrc.nist.gov/checklists> or by contacting John Wack, National Institute of Standards and Technology, Building 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930; telephone 301-975-3411; Fax 301-948-0279, or e-mail: checklists@nist.gov.

SUPPLEMENTARY INFORMATION:

NIST will lead an effort in coordination with other agencies and private industry to develop and disseminate a standard template designed to describe security checklists. Examples of key IT product technology areas include: operating systems, database systems, web servers, e-mail servers, firewalls, routers, intrusion detection systems, virtual private Networks, biometric devices, smart cards, telecommunication switching devices and web browsers.

Vendors, agencies, consortia, and other reputable sources will be encouraged to submit checklists and related information called for by the template to populate a public web-based repository. The template will provide a standardized method of centrally cataloging, describing, and categorizing existing and newly developed security checklists for IT products. The XML template will be used to populate an online database hosted by NIST that will provide the USG and Internet community with a centralized database used to consolidate information about IT product security checklists.

The initial workshop is being held to identify the key fields of the template. Workshop topics are planned to include:

- Target environments,
- Risk levels,
- Methods to gain wide agency and vendor support,
- Methods and incentives to encourage vendors' submissions adhering to the proposed template.

Vendors, agencies, and other reputable sources currently developing checklists for IT products are encouraged to present information at the workshop describing their checklist development and testing process. Speakers wishing to formally present information at the workshop should submit proposals to checklists@nist.gov by September 1, 2003.

Because of NIST security regulations, advance registration is mandatory; there

will be no on-site, same-day registration. To register, please register via the Web at <http://www.nist.gov/conferences> or fax the registration form with your name, address, telephone, fax and e-mail address to 301-948-2067 (Attn: Workshop on Building Secure Configurations/Security Settings/Security Checklists for Federal Government Systems) by September 22, 2003. The registration fee will be \$85. Payment can be made by credit card, check, purchase order, and government training form. Registration questions should be addressed to Kimberly Snouffer on 301-975-2776 or kimberly.snouffer@nist.gov.

Authority

This work effort is being initiated pursuant to NIST's responsibilities under the Cyber Security Research and Development Act of 2002.

Dated: July 7, 2003.

Arden L. Bement, Jr.,

Director.

[FR Doc. 03-17635 Filed 7-10-03; 8:45 am]

BILLING CODE 3510-13-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 021203A]

Small Takes of Marine Mammals Incidental to Specified Activities; Oceanographic Surveys in the Hess Deep, Eastern Equatorial Pacific Ocean

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of issuance of an incidental harassment authorization.

SUMMARY: In accordance with provisions of the Marine Mammal Protection Act (MMPA) as amended, notification is hereby given that an Incidental Harassment Authorization (IHA) to take small numbers of marine mammals, by harassment, incidental to conducting oceanographic surveys in the Hess Deep in international waters of the Eastern Equatorial Pacific Ocean has been issued to Lamont-Doherty Earth Observatory (L-DEO).

DATES: Effective from July 3, 2003, through June 30, 2004.

ADDRESSES: The application, a list of references used in this document, and/or the IHA are available by writing to Kaja A. Brix, Acting Chief, Marine Mammal Conservation Division, Office of Protected Resources, National Marine