

## 1999 FALL MEETING—REPORT ON PROPOSALS

[P=Partial revision; W=Withdrawal; R=Reconfirmation; N=New; C=Complete Revision]

Doc No.	Title	Action
1	Fire Prevention Code	C
12	Standard on Carbon Dioxide Extinguishing Systems	P
13E	Guide for Fire Department Operations in Properties Protected by Sprinkler and Standpipe Systems	C
14	Standard for the Installation of Standpipe and Hose Systems	P
70E	Standard for Electrical Safety Requirements for Employee Workplaces	P
97	Standard Glossary of Terms Relating to Chimneys, Vents and Heat-Producing Appliances	R
101	Code for Safety to Life from Fire in Buildings and Structures	P
102	Standard for Grandstands, Folding and Telescopic Seating, Tents, and Membrane Structures	W
130	Standard for Fixed Guideway Transit Systems	P
211	Standard for Chimneys, Fireplaces, Vents, and Solid Fuel-Burning Appliances	P
253	Standard Method of Test for Critical Radiant Flux of Floor Covering Systems Using a Radiant Heat Energy Source.	R
255	Standard Method of Test of Surface Burning Characteristics of Building Materials	P
257	Standard for Fire Test for Window and Glass Block Assemblies	C
269	Standard Test Method for Developing Toxic Potency Data for Use in Fire Hazard Modeling	R
286	Standard Method of Test for Room Corner Procedures	N
291	Recommended Practice for Fire Flow Testing and Marking of Hydrants	W
385	Standard for Tank Vehicles for Flammable and Combustible Liquids	P
386	Standard for Portable Shipping Tanks for Flammable and Combustible Liquids	W
430	Code for the Storage of Liquid and Solid Oxidizers	C
600	Standard on Industrial Fire Brigades	P
601	Standard for Security Services in Fire Loss Prevention	P
750	Standard on Water Mist Fire Protection Systems	P
850	Recommended Practice for Fire Protection for Electric Generating Plants and High Voltage Direct Current Converter Stations.	P
851	Recommended Practice for Fire Protection for Hydroelectric Generating Plants	P
1003	Standard for Airport Fire Fighter Professional Qualifications	C
1006	Standard for Rescue Technician Professional Qualifications	N
1035	Standard for Professional Qualifications for Public Fire and Life Safety Educator	C
1201	Standard for Developing Fire Protection Services for the Public	R
1250	Recommended Practice in Emergency Service Organization Risk Management	N
1410	Standard for Training for Initial Fire Attack	C
1452	Guide for Training Fire Service Personnel to Make Dwelling Fire Safety Surveys	C
1561	Standard on Fire Department Incident Management System	C
1581	Standard on Fire Department Infection Control Program	C
1582	Standard on Medical Requirements for Fire Fighters	C
1583	Recommended Practice for Fire Fighter Health and Wellness	N
1600	Recommended Practice for Disaster Management	C
1971	Standard on Protective Ensemble for Structural Fire Fighting	C
1976	Standard on Protective Clothing for Proximity Fire Fighting	C
1991	Standard on Vapor-Protective Suits for Hazardous Chemical Emergencies	C
1992	Standard on Liquid Splash-Protective Suits for Hazardous Chemical Emergencies	C
1993	Standard on Support Function Protective Clothing for Hazardous Chemical Operations	W

[FR Doc. 99-3716 Filed 2-16-99; 8:45 am]

BILLING CODE 3510-13-M

**DEPARTMENT OF COMMERCE****National Institute of Standards and Technology**

[Docket No. 981029270-8270-01]

**National Voluntary Laboratory Accreditation Program****AGENCY:** National Institute of Standards and Technology (NIST), Commerce.**ACTION:** Notice.

**SUMMARY:** The National Institute of Standards and Technology (NIST) has received a request to establish a laboratory accreditation program. In a letter dated August 5, 1998, the National Information Assurance Partnership

(NIAP), a partnership between NIST and the National Security Agency, requested that NIST establish an accreditation program for Information Technology Security Testing. A report of the request letter is set out as an appendix to this notice. Announcement of this request by NIAP and of the NIST request for comments with respect thereto, are being made under the procedures of the National Voluntary Laboratory Accreditation Program (NVLAP) [15 CFR 285.13] of the referenced procedures.

**DATES:** Comments may be submitted on or before May 3, 1999.

**ADDRESSES:** Comments should be submitted to James L. Cigler, Chief, Laboratory Accreditation Program, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2140, Gaithersburg, Maryland 20899-

2140. Copies of comments received will be available for inspection and copying at the Department of Commerce Central Reference and Records Inspections Facility, Room 6204, Hoover Building, Washington, DC 20230.

**FOR FURTHER INFORMATION CONTACT:** James L. Cigler, telephone 301-975-4016; e-mail james.cigler@nist.gov; <<http://ts.nist.gov/nvlap>>.

**SUPPLEMENTARY INFORMATION:****Background***Scope of Laboratory Accreditation*

The requestor referenced two documents to be used in association with accreditation of Information Technology (IT) Security Testing laboratories: (1) ISO/IEC DIS 15408 Information technology—Security techniques—Evaluation criteria for IT

Security also called the Common Criteria for Information Technology Security Evaluation, and (2) Common Evaluation Methodology for Information Security (CEM), an international draft. NVLAP currently offers accreditation for laboratories conducting testing to Federal Information Processing Standard (FIPS) 140-1 for Cryptographic Modules. Information about the Common Criteria and the Common Evaluation Methodology is available at <<http://csrc.nist.gov/cc/ccv20/ccv2list.htm>>.

After the 75-day comment period, NIST will thoroughly evaluate all comments pertaining to the proposed accreditation program and publish in the **Federal Register** an announcement of the decision of the Director of NIST, regarding development of the program. Those who submit comments and those who request future information will be placed on the NVLAP mailing list to receive a copy of that publication. If the decision is made to develop the program, technical assistance and input will be sought from all interested parties. Assistance will be sought in the areas of: (1) Preparation of the technical criteria for the program, (2) establishment of the scope of the program based on the Common Criteria, and (3) development of appropriate proficiency testing programs. The NVLAP procedures also provide for public comment prior to publication of the final accreditation requirements.

Dated: February 8, 1999.

**Karen H. Brown,**  
*Deputy Director.*

**National Information Assurance Partnership**  
August 5, 1998.

Raymond G. Kramer,  
*Director, National Institute of Standards and Technology, Gaithersburg, MD 20899*

Dear Mr. Kammer: The National Information Assurance Partnership (NIAP), a partnership between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), requests the establishment of a National Voluntary Laboratory Accreditation Program (NVLAP) Laboratory Accreditation Program (LAP) for Information Technology (IT) Security Testing. The requested LAP will support the goals and objectives of both NIST and NSA in fulfilling their responsibilities in the area of computer and information systems security. This request is made in accordance with Title 15 Code of Federal Regulations Section 285.13.

NIST plays a vital role in protecting the security and integrity of information in computer systems in the public and private sectors. The Computer Security Act of 1987 (P.L. 100-235) reaffirmed NIST's leadership role in the federal government for the protection of unclassified information. NIST assists industry and government by

promoting and supporting better security planning, technology, awareness and training.

NSA provides information systems security programs to protect classified and unclassified national security systems against exploitation through interception, unauthorized access, and related technical intelligence threats.

In a recent move to assist U.S. information security technology producers in achieving international competitiveness, NIST and NSA signed a letter of partnership establishing the National Information Assurance Partnership (NIAP). NIST and NSA have established a program under NIAP to evaluate conformance of IT products to international standards. This program, called the Common Criteria Evaluation and Validation Scheme, will help consumers make informed choices when selecting commercial off-the-shelf products in the area IT security and will help producers of IT security products gain acceptance in the global marketplace.

The NIAP Common Criteria Scheme requires IT security products to be tested in private sector, accredited testing laboratories using the test methods in ISO/IEC DIS 15408 (currently a Draft international standard), also called the Common Criteria, and the Common Evaluation Methodology (currently an international draft). Test reports from accredited laboratories will be reviewed by the NIAP Validation Body which will issue Common Criteria certificates for products that meet the NIAP Common Criteria Scheme requirements.

NIAP is working towards a Common Criteria Mutual Recognition Agreement with bodies in five foreign countries. By agreement, testing laboratories approved by the partners in each of the Agreement countries will be accredited as meeting the requirements of ISO/IEC Guide 25 by an organization that is internationally recognized as conforming to the requirements of ISO/IEC Guide 58.

NIST and NSA have been active participants in the development of the Common Criteria, the Common Evaluation Methodology, and the NIAP Common Criteria Scheme. NIST will provide technical assistance for the development of the LAP.

#### **Statement of Perceived Need**

The recent President's Commission on Critical Infrastructure Protection has pointed out that the United States is becoming increasingly dependent on information technology to carry out the day-to-day operations of business and government. This growing dependence on advanced technology, coupled with its inherent complexity, has introduced significant security vulnerabilities into the information systems that support the critical national infrastructure. Consumers within the public and private sectors are becoming increasingly aware of these vulnerabilities and are beginning to demand greater protection for their information from commercial IT products and systems.

As industry begins to respond to demands for security-enhanced IT products and systems, consumers must have confidence in

the security claims producers make about them. Testing at an accredited laboratory provides confidence to consumers in the test results and that the tested products and systems conform to the security criteria.

Acceptance of test results from a commercial laboratory by consumers in other nations and government organizations, such as those organizations in the countries participating in the Common Criteria project, requires trust and confidence in the laboratory testing processes. This trust and confidence is achieved through the use of accredited testing laboratories and government involvement in validating the results of commercial security evaluations. Thus, governments have greater confidence in the evaluation processes employed in the respective national schemes of other nations.

#### **Scope of the LAP, Applicable Standards, and Applicable Test Methods**

The scope of the proposed LAP includes conformance testing of commercial off-the-shelf, security-enhanced, IT products and systems to international standards. Applicable standards and test methods defined by government and industry will be employed by NVLAP-accredited testing laboratories operating within the scope of the LAP. Initially the score of the LAP will draw from, ISO/IEC DIS 15408 Information technology—Security techniques—Evaluation criteria for IT Security also called the Common Criteria for Information Technology Security Evaluation and Common Evaluation Methodology for Information Technology Security (CEM), an international draft. Additional standards and test methods may be added as they become available.

Evidence of a national need to accredit calibration or testing laboratories for the specific scope beyond that served by an existing laboratory accreditation program in the public or private sector.

The scope of the proposed LAP is beyond that served by any existing laboratory accreditation program in the public or private sector. The only commercial security testing laboratories currently available to conduct Common Criteria-based testing are the Trust Technology Assessment Program (TTAP) laboratories under a program established by the National Security Agency. These laboratories operate under cooperative research and development agreements (CRADA) with NSA and have not been accredited to ISO Guide 25. Recognition of evaluation results in the context of the nations participating in the Common Criteria project requires that IT products be evaluated at accredited testing laboratories. The unique nature of security testing and the associated knowledge and skills needed to operate an accreditation program in this area make NVLAP the essential choice to develop and implement the proposed LAP.

NIAP will hold public workshops to solicit comments on the Common Criteria Scheme and the proposed LAP from all sectors including producers, the testing laboratory community, and consumers of IT security products in the private and government sectors.

Sincerely,  
Stuart W. Katzke,  
Chief, Computer Security Division,  
Information Technology Laboratory NIST.

Louis F. Giles,  
Chief, Information Assurance Partnerships  
Evaluations, and Knowledge Management  
NSA.

cc: S. Wakid, Director, Information  
Technology Laboratory, NIST M. Jacobs,  
Deputy Director Information Systems  
Security, NSA

[FR Doc. 99-3718 Filed 2-16-99; 8:45 am]

BILLING CODE 3510-13-M

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

[I.D. 020899B]

#### Marine Mammals; File No. 772#69-03

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

**ACTION:** Issuance of permit amendment.

**SUMMARY:** Notice is hereby given that  
the Southwest Fisheries Science Center,  
National Marine Fisheries Service, 8604  
La Jolla shores Drive, La Jolla, CA 92038  
has been issued an amendment to  
scientific research Permit No. 1024 (File  
No. 772#69).

**ADDRESSES:** The amendment and related  
documents are available for review  
upon written request or by appointment  
in the following office(s):

Permits and Documentation Division,  
Office of Protected Resources, NMFS,  
1315 East-West Highway, Room 13705,  
Silver Spring, MD 20910 (301/713-  
2289);

Regional Administrator, Southwest  
Region, National Marine Fisheries  
Service, NOAA, 501 West Ocean Blvd.,  
Suite 4200, Long Beach, CA 90802-4213  
(562/980-4001).

**FOR FURTHER INFORMATION CONTACT:** Sara  
Shapiro or Ruth Johnson, 301/713-2289.

**SUPPLEMENTARY INFORMATION:** On  
January 5, 1999, notice was published in  
the **Federal Register** (64 FR 483) that an  
amendment of Permit No. 1024, issued  
December 30, 1996 (62 FR 1875), had  
been requested by the above-named  
organization. The requested amendment  
has been granted under the authority of  
the Marine Mammal Protection Act of  
1972, as amended (16 U.S.C. 1361 *et*  
*seq.*), the provisions of § 216.39 of the  
Regulations Governing the Taking and  
Importing of Marine Mammals (50 CFR  
part 216), and the Fur Seal Act of 1966,  
as amended (16 U.S.C. 1151 *et seq.*).

Permit No. 1024 authorizes the permit  
holder to conduct level B harassment  
activities [*i.e.* censuses] on, capture,  
handle, and release Antarctic pinnipeds  
in the South Shetland Islands,  
Antarctica. The holder is now  
authorized to increase the number of  
Antarctic fur seal (*Arctocephalus*  
*gazella*) pups and juveniles to be  
captured and handled for oxygen  
consumption and developmental  
physiology studies. The Holder will  
conduct these activities at Cape Shirreff  
on Livingston Island, Antarctica.

Dated: February 11, 1999.

**E. Ruth Johnson,**

*Acting Chief, Permits and Documentation  
Division, Office of Protected Resources,  
National Marine Fisheries Service.*

[FR Doc. 99-3848 Filed 2-16-99; 8:45 am]

BILLING CODE 3510-22-F

## DEPARTMENT OF DEFENSE

### Department of the Air Force

#### Notice of Intent To Prepare an Environmental Impact Statement To Convert Two F-15 Formal Training Units to F-22 Units at Tyndall Air Force Base, Florida

The United States Congress has  
determined the need exists to phase the  
older F-15 aircraft out of the primary air  
superiority role. The F-22 "Raptor" has  
been chosen as the replacement aircraft  
to fulfill future combat air superiority  
requirements. Therefore, the United  
States Air Force (USAF) is announcing  
its intent to prepare an Environmental  
Impact Statement (EIS) to assess the  
potential environmental impacts of  
converting two of the three existing  
formal training units (FTUs) at Tyndall  
Air Force Base (AFB), Florida from F-  
15s to F-22s. This action will be known  
as the F-22 Conversion EIS.

Tyndall AFB currently supports  
training for the majority of USAF F-15  
air-to-air pilots. It currently supports 87  
aircraft, three FTUs, and 4,600 support  
personnel. In addition, it supports 1,625  
additional personnel assigned to 29  
associated units.

The USAF proposes conversion over  
a 5-year period starting in 2003. During  
this period, the total number of aircraft  
will increase from 78 to 105 at the peak  
(in 2008). From 2008 through 2012, the  
number of F-15s will be reduced to a  
single squadron of 28 aircraft. The total  
number of F-22s will remain constant  
after 2008 with 60 in two squadrons.  
This proposed action includes training  
of student pilots, instructor fighter  
pilots, and ground crews. It will also  
provide for construction, modification

and/or use of operational and training  
facilities (academic facility, simulator,  
etc.), base operating support (housing,  
commissary, etc.), logistics support  
(maintenance facilities, supply,  
transportation), and the necessary  
military airspace to conduct the  
required training.

Because of the increased maneuvering  
capabilities of the F-22 over the F-15,  
additional military airspace is needed  
for pilot training. Currently, Tyndall  
AFB's most frequently used military  
airspace is over water approximately 50  
miles southeast of the base near St.  
George Island. This area is called  
Warning Area-470, or simply W-470. A  
nonregulatory Warning Area (W) is  
airspace of defined dimensions  
designated over international waters  
that contains activity which may be  
hazardous to nonparticipating aircraft.  
The purpose of such warning areas is to  
warn nonparticipating pilots of the  
potential danger.

W-470 starts 3 nautical miles (nm)  
from land and extends south into the  
Gulf of Mexico approximately 100 nm.  
Less frequently, Tyndall AFB aircraft  
use the airspace called W-151 which  
lies over the Gulf of Mexico south of  
Eglin AFB that is approximately 100 nm  
out. Tyndall AFB aircraft also use over  
3,000 square miles of over-land military  
airspace for subsonic air-to-air training.  
The areas to the north, east, and  
southeast of the base are called the  
Tyndall Military Operating Areas  
(MOAs).

For supersonic training, the USAF  
proposes to maximize the use of W-470,  
to increase the frequency of use of W-  
151, and to add W-168 for unrestricted  
training. The W-168 airspace lies south  
and east of W-470, nearly 140 nm from  
St. George Island. It extends offshore  
from approximately Tampa to Ft.  
Meyers. For large-scale exercises and as  
an overflow training area, the USAF  
proposes use of the areas known as the  
Eglin Water Test Areas (EWTAs), which  
is airspace located further out in the  
Gulf, below W-151 and W-470.

The alternatives being considered  
include the mix of military airspace  
used for training and alternative  
locations for siting new facilities.  
Alternative airspace use includes: (1)  
Using the same airspace used by the F-  
15s (Tyndall overland areas, W-470,  
and W-151 on a limited basis),  
including recharting of the over water  
airspace to accommodate the larger area  
needed for the F-22s; (2) using the same  
airspace used by the F-15s, with regular  
use of W-168, increased use of W-151,  
and limited use of the EWTAs and W-  
155; and (3) using the same airspace  
used by the F-15s, with increased use