maker subject to prosecution under 18 U.S.C. 1001.

(End of provision)

1252.237–72 Prohibition on advertising.

As prescribed in (TAR) 48 CFR 1213.7101 and 1237.7003, insert the following clause:

PROHIBITION ON ADVERTISING (JAN 1996)

The contractor or its representatives (including training instructors) shall not advertise or solicit business from attendees for private, non-Government training during contracted-for training sessions. This prohibition extends to unsolicited oral comments, distribution or sales of written materials, and/or sales of promotional videos or audio tapes. The contractor agrees to insert this clause in its subcontracts.

(End of clause)

1252.237–73 Key personnel.

As prescribed in (TAR) 48 CFR 1237.110(b), insert the following clause:

KEY PERSONNEL (APR 2005)

(a) The personnel as specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel, as appropriate.

(b) Before removing, replacing, or diverting any of the specified individuals, the Contractor shall notify the contracting officer, in writing, before the change becomes effective. The Contractor shall submit information to support the proposed action to enable the contracting officer to evaluate the potential impact of the change on the contract. The Contractor shall not remove or replace personnel under this contract until the Contracting Officer approves the change.

The Key Personnel under this Contract are: (*specify key personnel*)

(End of clause)

1252.239–70 Security requirements for unclassified information technology resources.

As prescribed in (TAR) 48 CFR 1239.70, insert the following clause:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (APR 2005)

(a) The Contractor shall be responsible for Information Technology security for all systems connected to a Department of Transportation (DOT) network or operated by the Contractor for DOT, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to DOT's sensitive information that directly supports the mission of DOT. The term ''information technology,'' as used in this clause, means any equipment or interconnected system or subsystem of equipment, including telecommunications equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes both major applications and general support systems as defined by OMB Circular A–130. Examples of tasks that require security provisions include:

(1) Hosting of DOT e-Government sites or other IT operations;

(2) Acquisition, transmission or analysis of data owned by DOT with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to DOT general support systems/major applications at a level beyond that granted the general public, e.g. bypassing a firewall.

(b) The Contractor shall develop, provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002 and the E-Government Act of 2002. The plan shall meet IT security requirements in accordance with Federal and DOT policies and procedures, as they may be amended from time to time during the term of this contract that include, but are not limited to:

(1) OMB Circular A–130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources;

(2) National Institute of Standards and Technology (NIST) Guidelines;

(3) Departmental Information Resource Management Manual (DIRMM) and associated guidelines; and

(4) DOT Order 1630.2B, Personnel Security Management

(c) Within 30 days after contract award, the contractor shall submit the IT Security Plan to the DOT Contracting Officer for acceptance. This plan shall be consistent with and further detail the approach contained in

the offeror's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

(d) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to the DOT for acceptance by the DOT Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. Accreditation must be in accordance with DOT Order 1350.2, which is available from the Contracting Officer upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document, and shall include a final security plan, a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan. The contractor shall comply with the accepted accreditation documentation.

(e) On an annual basis, the contractor shall submit verification to the Contracting Officer that the IT Security Plan remains valid.

(f) The contractor will ensure that the following banners are displayed on all DOT systems (both public and private) operated by the contractor prior to allowing anyone access to the system:

GOVERNMENT WARNING

WARNINGWARNING**WARNING**

Unauthorized access is a violation of U.S. Law and Department of Transportation policy, and may result in criminal or administrative penalties. Users shall not access other user's or system files without proper authority. Absence of access controls IS NOT authorization for access! DOT information systems and related equipment are intended for communication, transmission, processing and storage of U.S. Government information. These systems and equipment are subject to monitoring by law enforcement and authorized Department officials. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored in this system by law enforcement and authorized Department officials. Use of this system constitutes consent to such monitoring.

WARNINGWARNING**WARNING**

(g) The contractor will ensure that the following banner is displayed on all DOT systems that contain Privacy Act information operated by the contractor prior to allowing anyone access to the system:

This system contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93–579). Any privacy information displayed on the screen or printed shall be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary actions, a fine of up to $5,000, or both.

(h) Contractor personnel requiring privileged access or limited privileged access to systems operated by the Contractor for DOT or interconnected to a DOT network shall be screened at an appropriate level in accordance with DOT Order 1630.2B, Personnel Security Management, as it may be amended from time to time during the term of this contract.

(i) The Contractor shall ensure that its employees, in performance of the contract performing under this contract, receive annual IT security training in accordance with OMB Circular A–130, FISMA, and NIST requirements, as they may be amended from time to time during the term of this contract, with a specific emphasis on rules of behavior.

(j) The Contractor shall afford the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection (to include vulnerability testing), investigation and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DOT data or to the function of information technology systems operated on behalf of DOT, and to preserve evidence of computer crime.

(k) The Contractor shall incorporate the substance of this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(l) The contractor shall immediately notify the contracting officer when an employee terminates employment that has access to DOT information systems or data.

(End of clause)

1252.239–71 Information technology security plan and accreditation.

As prescribed in (TAR) 48 CFR 1239.70, insert the following provision:

INFORMATION TECHNOLOGY SECURITY PLAN AND ACCREDITATION (APR 2005)

All offers submitted in response to this solicitation must address the approach for completing the security plan and accreditation requirements in TAR clause 1252.239–70.