552.239–70 Information Technology Security Plan and Security Authorization

As prescribed in 539.7002(a), insert the following provision:

**INFORMATION TECHNOLOGY SECURITY PLAN AND SECURITY AUTHORIZATION (JUN 2011)**

All offers/bids submitted in response to this solicitation must address the approach for completing the security plan and certification and security authorization requirements as required by the clause at 552.239–71, Security Requirements for Unclassified Information Technology Resources.

(End of provision)

[76 FR 34888, June 15, 2011]

552.239–71 Security Requirements for Unclassified Information Technology Resources

As prescribed in 539.7002(b), insert the following clause:

**SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2011)**

(a) General. The Contractor shall be responsible for information technology (IT) security, based on General Services Administration (GSA) risk assessments, for all systems connected to a GSA network or operated by the Contractor for GSA, 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 GSA’s information that directly supports the mission of GSA, as indicated by GSA. The term information technology, as used in this clause, means any equipment, including telecommunications equipment that is used in the automatic acquisition, storage, manipulation, management, control, display, switching, interchange, transmission, or reception of data or information. This includes major applications as defined by OMB Circular A–130. Examples of tasks that require security provisions include:

1. Hosting of GSA e-Government sites or other IT operations;
2. Acquisition, transmission, or analysis of data owned by GSA with significant replacement cost should the Contractors copy be corrupted;
3. Access to GSA major applications at a level beyond that granted the general public; e.g., bypassing a firewall; and
4. Any new information technology systems acquired for operations within the GSA must comply with the requirements of HSPD–12 and OMB M–11–11. Usage of the credentials must be implemented in accordance with OMB policy and NIST guidelines (e.g., NIST SP 800-116). The system must operate within the GSA’s access management environment. Exceptions must be requested in...