the HSAR. Component desiring to use a provision or a clause on a standard basis shall submit a request containing a copy of the clause(s), justification for its use, and evidence of legal counsel review to the CPO in accordance with (HSAR) 48 CFR 3001.304 for possible inclusion in the HSAR.

(B) Provisions and clauses used on a one-time basis (i.e., non-standard provisions and clauses) may be approved by the contracting officer, unless a higher level is designated by the Component. This authority is subject to:

(1) Evidence of legal counsel review in the contract file;
(2) Inserting these clauses in the appropriate sections of the uniform contract format; and
(3) Ensuring the provisions and clauses do not deviate from the requirements of the FAR and HSAR.


Subpart 3052.2—Text of Provisions and Clauses

3052.203–70 Instructions for Contractor Disclosure of Violations.

As prescribed in (HSAR) 48 CFR 3003.1004(a), insert the following clause:

INSTRUCTIONS FOR CONTRACTOR DISCLOSURE OF VIOLATIONS (SEP 2012)

When making a written disclosure under the clause at FAR 52.203–13, paragraph (b)(3), the Contractor shall use the Contractor Disclosure Form at [http://www.oig.dhs.gov](http://www.oig.dhs.gov) and submit the disclosure electronically to the Department of Homeland Security Office of Inspector General. The Contractor shall provide a copy of the disclosure to the Contracting Officer by email or facsimile on the same business day as the submission to the Office of Inspector General. The Contractor shall provide the Contracting Officer a concurrent copy of any supporting materials submitted to the Office of Inspector General.

[77 FR 54836, Sept. 6, 2012]
Homeland Security Department

3052.204–71 Contractor employee access.

As prescribed in (HSAR) 48 CFR 3004.470–3(b), insert a clause substantially the same as follows with appropriate alternates:

**CONTRACTOR EMPLOYEE ACCESS (SEP 2012)**

(a) Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals, including, but not limited to, careless or contrary to the public interest for any reason.

(b) Information Technology Resources include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer’s request, the Contractor’s employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that