AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

defense information. None of the restrictions on the Government's use or sharing of information under the DIB CS/IA program shall limit the Government's ability to conduct law enforcement, counterintelligence activities, or other activities in the interest of national security; and participation does not supersede other regulatory or statutory requirements.

(e) Participation in the DIB CS/IA program is voluntary and does not obligate the DIB participant to utilize the GFI in, or otherwise to implement any changes to, its information systems. Any action taken by the DIB participant based on the GFI or other participation in this program is taken on the DIB participant's own volition and at its own risk and expense.

(f) A DIB participant's voluntary participation in this program is not intended to create any unfair competitive advantage or disadvantage in DoD source selections or competitions, or to provide any other form of unfair preferential treatment, and shall not in any way be represented or interpreted as a Government endorsement or approval of the DIB participant, its information systems, or its products or services.

(g) The DIB participant and the Government may each unilaterally limit or discontinue participation in this program at any time. Termination shall not relieve the DIB participant or the Government from obligations to continue to protect against the unauthorized use or disclosure of GFI, attribution information, contractor proprietary information, third-party proprietary information, or any other information exchanged under this program, as required by law, regulation, contract, or the FA.

(h) Upon termination of the FA, and/or change of Facility Security Clearance status below Secret, GFI must be returned to the Government or destroyed pursuant to direction of, and at the discretion of, the Government.

(i) Participation in this program does not abrogate the Government's or the DIB participants' rights or obligations regarding the handling, safeguarding, sharing, or reporting of information, or regarding any physical, personnel, or other security requirements, as required by law, regulation, policy, or a valid legal contractual obligation.

§236.7 DIB participant eligibility requirements.

To be eligible to participate in this program, a DIB company must:

(a) Have or acquire DoD-approved medium assurance certificates to enable encrypted unclassified information sharing between the Government and DIB participants;

(b) Have an existing active Facility Security Clearance (FCL) granted under the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22–M) with approved safeguarding for at least Secret information, and continue to qualify under the NISPOM for retention of its FCL and approved safeguarding (*http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf*);

(c) Have or acquire a Communication Security (COMSEC) account in accordance with the NISPOM Chapter 9, Section 4 (DoD 5220.22–M), which provides procedures and requirements for COMSEC activities;

(d) Obtain access to DoD's secure voice and data transmission systems supporting the DIB CS/IA program,

(e) Own or operate covered DIB system(s), and

(f) Execute the standardized FA with the Government (available during the application process), which implements the requirements set forth in §§236.4 through 236.6.

PART 237a—PUBLIC AFFAIRS LIAISON WITH INDUSTRY

Sec.
237a.1 Purpose.
237a.2 Applicability.
237a.3 Objective and policy.
237a.4 Procedures.

AUTHORITY: 5 U.S.C. 301.

SOURCE: 35 FR 10889, July 7, 1970, unless otherwise noted.

§237a.1 Purpose.

This part establishes (a) guidance for preparation of the Defense Industry Bulletin, and (b) includes guidance and procedures governing Department of Defense cooperation with industry on (1) public affairs matters in general, (2)