§ 2004.10 Responsibilities of the Director, Information Security Oversight Office (ISOO) [102(b)].

The Director ISOO shall:
(a) Implement EO 12829, as amended.
(b) Ensure that the NISP is operated as a single, integrated program across the Executive Branch of the Federal Government; i.e., that the Executive Branch departments and agencies adhere to NISP principles.
(c) Ensure that each contractor’s implementation of the NISP is overseen by a single Cognizant Security Authority (CSA), based on a preponderance of classified contracts per agreement by the CSAs.
(d) Ensure that all Executive Branch departments and agencies that contract for classified work have included the Security Requirements clause, 52.204–2, from the Federal Acquisition Regulation (FAR), or an equivalent clause, in such contract.
(e) Ensure that those Executive Branch departments and agencies for which the Department of Defense (DoD) serves as the CSA have entered into agreements with the DoD that establish the terms of the Secretary’s responsibilities on behalf of those agency heads.

§ 2004.11 Agency Implementing Regulations, Internal Rules, or Guidelines [102(b)(3)].

(a) Reviews and Updates. All implementing regulations, internal rules, or guidelines that pertain to the NISP shall be reviewed and updated by the originating agency, as circumstances require. If a change in national policy necessitates a change in agency implementing regulations, internal rules, or guidelines that pertain to the NISP, the agency shall promptly issue revisions.
(b) Reviews by ISOO. The Director, ISOO, shall review agency imple-