COMMENTS ON ISOO DRAFT REVISION
OF EXECUTIVE ORDER 12065

A. Page 7, Section 1-302

Change to read "Information that is determined to concern one or more of the categories in Section 1-301 shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security."

As presently drafted, the consideration of information in the context of other related information is limited to fitting that information into a classification category under Section 1-301 rather than satisfying the damage or harm standard of Section 1-302 itself. The importance of permitting agencies to consider this "aggregate" effect in classifying information is to enable agencies to realistically assess the potential damage of disclosure. As amended, this section now authorizes agencies to consider the disclosure of related information in making this damage determination.

B. Page 8, Section 1-303

Change to read "Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or information relating to intelligence activities (including special activities), or intelligence sources or methods, is presumed to cause damage to the national security."

The addition of "intelligence activities (including special activities)" is consistent with similar constructions throughout the draft.

C. Page 9, Section 1-501

Move the parenthetical provision in 1-501(a) and 1-501(b) to the main paragraph of 1-501, where it appeared in a previous draft.

This marking exclusion must appear in the main paragraph in order to cover all markings. There are circumstances in which any type of U.S. marking would reveal a confidential relationship.

D. Page 16, Section 3-301

The last sentence of Section 3-301 should be separated and made into a new Section 3-303. Additionally, the last five words of this sentence should be deleted.

This provision for establishing special Secretary of Defense and DCI review procedures should be separate to make clear that the procedures may apply to all agencies, not just the National Archives. In establishing these procedures, mandatory consultation with affected agencies should not be required (even though such consultation normally occurs).

E. Page 18, Section 3-402

Restructure the first two sentences to read: "Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provision of Section 3-401. The Archivist of the United States shall have authority to review and declassify such information in the possession and control of the Administrator of General Services pursuant to Sections 2107, 2107 note, or 2203 of Title 44 U.S.C."

This is consistent with the coverage of Archivist authority provided elsewhere in the draft, which authority includes only that information in GSA custody.

F. Page 19, Section 3-404

The fourth sentence of Section 3-404 should be separated and numbered Section 3-405. The present Section 3-405 should be renumbered 3-406.

As with Section 3-301 (comment D above), the provision covering special Secretary of Defense and DCI review procedures should be separated to indicate that these procedures have general effect. The addition of the new authority for Archivist review in Section 3-402 (comment E above) also requires that this provision be separated to make clear that it is not tied solely to the "mandatory review" provision of Section 3-404.

G. Page 22, Section 4-202

Delete entire section.

This requirement is unclear, unnecessary, burdensome and has failed to work in present Executive Order 12065.

H. Page 28, Section 5-402

Change the introductory clause of Section 5-402 to read "Appropriate sanctions may be applied to any person who..."

Under the present draft, the application of sanctions is limited to "officers or employees of the United States Government" who commit any of the enumerated acts. Appropriate sanctions should also be authorized against non-employees who are provided access to classified information and violate the terms of the Order. This would explicitly authorize agencies to take any action "in accordance with applicable law and agency regulation" as provided in Section 5-403, including the termination of present and denial or future access to such classified information by non-employees.

I. Page 28, Section 5-403

Add the following language: "Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanction..."

The Order should explicitly state that a loss of current access to classified information, or a denial of requested access at some future date are appropriate sanctions for violations of the Order. This is particularly true in the case of contractor personnel and other individuals who are not "employees" and thus not subject to many of the other authorized sanctions.

J. Page 29, Section 5-404

Change the last sentence to read "Either shall ensure that the Director of the Information Security Oversight Office is informed periodically of violations under Section 5-402(a) or (b)."

Notifying D/ISOO on each occasion when there is an improper disclosure of classified information could adversely impact the Agency's polygraph program. Periodic notification of such violations will permit ISOO to fully perform its oversight function in this area.

K. Page 31, add Section 6-108

6-108. "Cryptology," for the purposes of this Order, means cryptography and communications security.

This definition reflects the current Intelligence Community understanding that the Director of Central Intelligence is responsible for the portion of intelligence sources and methods known as signals intelligence (SIGINT) and the Secretary of Defense is responsible for communications security (COMSEC) matters. Without this definition, Section 4-201 of the ISOO draft is in direct contravention to the statutory authority of the DCI. Furthermore, NSCID 6 specifically makes the DCI responsible for SIGINT security policy. According to the official, current, Intelligence Community Glossary of Intelligence terms, "cryptology" includes both SIGINT and COMSEC. As an alternative to the addition of a definition for "cryptology," the word "cryptography" or "cryptographic" might be substituted for "cryptology" or "cryptologic" throughout the ISOO draft.

L. In addition to the above comments, we support the ISOO wording changes in Sections 1-101(a), 1-103, 1-204(e), 1-205, 1-303, 1-501, 2-102(b), 3-401(b), 3-404, 5-202(d), 5-202(g), 5-301(b), 5-402(a), and 6-106. Further, we do not object to the changes in Sections 1-301(j), 1-401, 1-402, 1-501(c), 3-203, 3-401(a), 3-403, 3-405(b), 4-101, 5-102, 5-301(c), and 6-107. Also, there are two typographical errors in the last sentence of Section 3-301. There is an extra comma preceding the parenthesis in this sentence, and "sources and methods" should read "sources or methods." Additionally, the "could reasonably" in Section 6-106 should read "reasonably could."