Section 3. Reporting Requirements

1-300. General. Contractors are required to report certain events that: impact the status of the facility clearance (FCL); impact the status of an employee's personnel security clearance (PCL); may indicate the employee poses an insider threat; affect proper safeguarding of classified information, or that indicate classified information has been lost or compromised.

a. Contractors shall establish such internal procedures as are necessary to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the FSO, the Federal Bureau of Investigation (FBI), or other Federal authorities as required by this Manual, the terms of a classified contract, and U.S. law. Contractors shall provide complete information to enable the CSA to ascertain whether classified information is adequately protected. Contractors shall submit reports to the FBI and to their CSA as specified in this section.

b. When the reports are classified or offered in confidence and so marked by the contractor, the information will be reviewed by the CSA to determine whether it may be withheld from public disclosure under applicable exemptions of the Freedom of Information Act (5 U.S.C. 552) (reference (k)).

c. When the reports are unclassified and contain information pertaining to an individual, the Privacy Act of 1974 (5 U.S.C. 552a)(reference (l)) permits withholding of that information from the individual only to the extent that the disclosure of the information would reveal the identity of a source who furnished the information to the U.S. Government under an expressed promise that the identity of the source would be held in confidence. The fact that a report is submitted in confidence must be clearly marked on the report.

1-301. Reports to be Submitted to the FBI. The contractor shall promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations. An initial report may be made by phone, but it must be followed in writing, regardless of the disposition made of the report by the FBI. A copy of the written report shall be provided to the CSA.

1-302. Reports to be Submitted to the CSA

a. Adverse Information. Contractors shall report adverse information coming to their attention concerning any of their cleared employees. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. If the individual is employed on a Federal installation, the contractor shall furnish a copy of the report and its final disposition to the commander or head of the installation.

NOTE: In Taglia vs. Philco (372 F.2d 771), the U.S. Court of Appeals for the 4th Circuit decided that a contractor is not liable for defamation of an employee because of reports made to the Government under the requirements of this Manual and its previous versions. In Becker v. Philco (389 U.S. 979), the U.S. Supreme Court denied the appeal from the 4th Circuit.

b. Suspicious Contacts. Contractors shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country shall be reported.

c. Change in Cleared Employee Status. Contractors shall report: (1) the death; (2) a change in name; (3) the termination of employment; (4) change in citizenship; and (5) when the possibility of access to classified information in the future has been reasonably foreclosed. The CSA shall designate the appropriate reporting mechanism.

d. Citizenship by Naturalization. Contractors shall report if a non-U.S. citizen employee granted a Limited Access Authorization (LAA) becomes a citizen through naturalization. The report shall include: (1) city, county, and state where naturalized; (2) date naturalized; (3) court; and (4) certificate number.

e. Employees Desiring Not to Perform on Classified Work. Contractors shall report that an employee no longer wishes to be processed for a clearance or to continue an existing clearance.

f. Standard Form (SF) 312. Refusal by an employee to execute the "Classified Information Nondisclosure Agreement" (SF 312).

g. Change Conditions Affecting the Facility Clearance

(1) Any change of ownership, including stock transfers that affect control of the company.

(2) Any change of operating name or address of the company or any of its cleared locations.

(3) Any change to the information previously submitted for key management personnel including, as appropriate, the names of the individuals they are replacing. In addition, a statement shall be made indicating (a) whether the new key management personnel are cleared, and if so, to what level and when, their dates and places of birth, social security numbers, and their citizenship; (b) whether they have been excluded from access; or (c) whether they have been temporarily excluded from access pending the granting of their clearance. A new complete listing of key management personnel need be submitted only at the discretion of the contractor and/or when requested by the CSA.

(4) Action to terminate business or operations for any reason, imminent adjudication or reorganization in bankruptcy, or any change that might affect the validity of the FCL.

(5) Any material change concerning the information previously reported by the contractor concerning foreign ownership, control or influence (FOCI). This report shall be made by the submission of a Certificate Pertaining to Foreign Interests. When submitting this information, it is not necessary to repeat answers that have not changed. When entering into discussions, consultations or agreements that may reasonably lead to effective ownership or control by a foreign interest, the contractor shall report the details by letter. If the contractor has received a Schedule 13D from the investor, a copy shall be forwarded with the report.

h. Changes in Storage Capability. Any change in the storage capability that would raise or lower the level of classified information the facility is approved to safeguard.

i. Inability to Safeguard Classified Material. Any emergency situation that renders the facility incapable of safeguarding classified material.

j. Security Equipment Vulnerabilities. Significant vulnerabilities identified in security equipment, intrusion detection systems (IDS), access control systems, communications security (COMSEC) equipment or systems, and IS security hardware and software used to protect classified material.

k. Unauthorized Receipt of Classified Material. The receipt or discovery of any classified material that the contractor is not authorized to have. The report should identify the source of the material, originator, quantity, subject or title, date, and classification level.

l. Employee Information in Compromise Cases. When requested by the CSA, information concerning an employee when the information is needed in connection with the loss, compromise, or suspected compromise of classified information.

m. Disposition of Classified Material Terminated From Accountability. When the whereabouts or disposition of classified material previously terminated from accountability is subsequently determined.

n. Foreign Classified Contracts. Any precontract negotiation or award not placed through a GCA that involves, or may involve: (1) the release or disclosure of U.S. classified information to a foreign interest or (2) access to classified information furnished by a foreign interest.

1-303. Reports of Loss, Compromise, or Suspected Compromise. Any loss, compromise or suspected compromise of classified information, foreign or domestic, shall be reported to the CSA. Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise. If the facility is located on a Government installation, the report shall be furnished to the CSA through the Commander or Head of the host installation.

a. Preliminary Inquiry. Immediately on receipt of a report of loss, compromise, or suspected compromise of classified information, the contractor shall initiate a preliminary inquiry to ascertain all of the circumstances surrounding the reported loss, compromise or suspected compromise.

b. Initial Report. If the contractor's preliminary inquiry confirms that a loss, compromise, or suspected compromise of any classified information occurred, the contractor shall promptly

submit an initial report of the incident unless otherwise notified by the CSA. Submission of the initial report shall not be deferred.

c. Final Report. When the investigation has been completed, a final report shall be submitted to the CSA. The report should include:

(1) Material and relevant information that was not included in the initial report;

(2) The name and social security number of the individual(s) who was primarily responsible for the incident, including a record of prior loss, compromise, or suspected compromise for which the individual had been determined responsible;

(3) A statement of the corrective action taken to preclude a recurrence and the disciplinary action taken against the responsible individual(s), if any; and

(4) Specific reasons for reaching the conclusion that loss, compromise, or suspected compromise occurred or did not occur.

1-304. Individual Culpability Reports. Contractors shall establish and enforce policies that provide for appropriate administrative actions taken against employees who violate requirements of this Manual. They shall establish and apply a graduated scale of disciplinary actions in the event of employee violations or negligence. A statement of the administrative actions taken against an employee shall be included in a report to the CSA when individual responsibility for a security violation can be determined and one or more of the following factors are evident:

a. The violation involved a deliberate disregard of security requirements.

b. The violation involved gross negligence in the handling of classified material.

c. The violation involved was not deliberate in nature but involves a pattern of negligence or carelessness.