APPENDIX B TO PART 327—INTERNAL MANAGEMENT CONTROL REVIEW CHECKLIST

Dear Mrs. Employee: This responds to your Privacy Act request dated (enter date of request), in which you requested (describe requested records).

Your request has been referred to our headquarters for further processing. They will respond directly to you. Any questions concerning your request may be made telephonically (enter Privacy Officer’s telephone number) or in writing to the following address:


I trust this information is responsive to your needs.

(Signature block)

APPENDIX B TO PART 327—INTERNAL MANAGEMENT CONTROL REVIEW CHECKLIST

(a) Task: Personnel and/or Organization Management.

(b) Subtask: Privacy Act (PA) Program.

(c) Organization:

(d) Action officer:

(e) Reviewer:

(f) Date completed:

(g) Assessable unit: The assessable units are HQ, DeCA, Regions, Central Distribution Centers, Field Operating Activities, and commissaries. Each test question is annotated to indicate which organization(s) is (are) responsible for responding to the question(s). Assessable unit managers responsible for completing this checklist are shown in the DeCA, MCP, DeCA Directive 70–2.1

(h) Event cycle 1: Establish and implement a Privacy Act Program.

(i) Risk: If prescribed policies, procedures and responsibilities of the Privacy Act Program are not adhered to, sensitive private information on individuals can be given out to individuals.

(j) Control Objectives: The prescribed policies, procedures and responsibilities contained in 5 U.S.C. 552a are followed to protect individual privacy and information release.


(l) Ensure that a PA program is established and implemented.

(m) Ensure that a PA program is established and implemented.

(n) Ensure that a PA program is established and implemented.

(o) Appoint an individual with PA responsibilities and ensure the designation of appropriate staff to assist.

(p) Test Questions: Explain rationale for YES responses or provide cross-references where rationale can be found. For NO responses, cross-reference to where corrective action plans can be found. If response is NA, explain rationale.

(i) Is a PA program established and implemented in DeCA to encompass procedures for subordinate activities? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(ii) Is an individual appointed PA responsibilities? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(iii) Are the current names and office telephone numbers furnished OSD, Private Act Office of the PA Officer and the IDA? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(iv) Is the annual PA report prepared and forwarded to OSD, Defense Privacy Office? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(v) Is PA awareness training/orientation provided? Is in-depth training provided for personnel involved in the establishment, development, custody, maintenance and use of a system of records? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(vi) Is the PA Officer consulted by information systems developers for privacy requirements which need to be included as part of the life cycle management of information considered in information systems design? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(vii) Is each system of records maintained by DeCA supported by a Privacy Act System Notice and has the systems notice been published in the Federal Register? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

1 Copies may be obtained: Defense Commissary Agency, ATTN: FOIA Privacy Officer, 1300 E. Avenue, Fort Lee, VA 23801–1800.

2 See footnote 1 to this Appendix B.
Office of the Secretary of Defense

Pt. 327, App. C

(1) Risk: Unprotected records allowing individuals without a need to know access to privacy information.
(2) Control Objective: PA records are properly maintained throughout their life cycle.
(3) Control Technique: Ensure the prescribed policies and procedures are followed during the life cycle of information.

(4) Test Questions:
(i) Are file cabinets/containers that house PA records locked at all times to prevent unauthorized access? (All). Response: Yes/No/NA. Remarks:
(ii) Are personnel with job requirement (need to know) only allowed access to PA information? (All). Response: Yes/No/NA. Remarks:
(iii) Are privacy act records treated as unclassified records and designated ‘For Official Use Only’? (All). Response: Yes/No/NA. Remarks:
(iv) Are computer printouts that contain privacy act information as well as disks, tapes and other media marked ’For Official Use Only’? (All). Response: Yes/No/NA. Remarks:
(v) Is a Systems Manager appointed for each automated/manual PA systems of records? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:
(vi) Are PA records maintained and disposed of in accordance with DeCA Directive 30-2. The Defense Commissary Agency Filing System? (All). Response: Yes/No/NA. Remarks:
(vii) Is coordination met with the General Counsel prior to forwarding a PA request to the IDA? (DeCA HQ/SA). Response: Yes/No/NA. Remarks:
(viii) Are privacy act records treated as unclassified records and designated ‘For Official Use Only’? (All). Response: Yes/No/NA. Remarks:
(ix) Are PA records maintained and disposed of in accordance with DeCA Directive 30-2. The Defense Commissary Agency Filing System? (All). Response: Yes/NO/NA. Remarks:
(x) Is a Systems Manager appointed for each automated/manual PA systems of records? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:
(xi) Are PA records maintained and disposed of in accordance with DeCA Directive 30-2. The Defense Commissary Agency Filing System? (All). Response: Yes/No/NA. Remarks:
(xii) Is a Systems Manager appointed for each automated/manual PA systems of records? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:
(xiii) Are privacy act records treated as unclassified records and designated ‘For Official Use Only’? (All). Response: Yes/No/NA. Remarks:
(xiv) Are computer printouts that contain privacy act information as well as disks, tapes and other media marked ’For Official Use Only’? (All). Response: Yes/No/NA. Remarks:
(xv) Is a Systems Manager appointed for each automated/manual PA systems of records? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:
(xvi) Are PA records maintained and disposed of in accordance with DeCA Directive 30-2. The Defense Commissary Agency Filing System? (All). Response: Yes/No/NA. Remarks:
(xvii) Is a Systems Manager appointed for each automated/manual PA systems of records? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:
(xviii) Are PA records maintained and disposed of in accordance with DeCA Directive 30-2. The Defense Commissary Agency Filing System? (All). Response: Yes/No/NA. Remarks:
(xix) Is a Systems Manager appointed for each automated/manual PA systems of records? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:
(xx) Are PA records maintained and disposed of in accordance with DeCA Directive 30-2. The Defense Commissary Agency Filing System? (All). Response: Yes/No/NA. Remarks:

APPENDIX C TO PART 327—DECA BLANKET ROUTINE USES

(a) Routine Use—Law Enforcement. If a system of records maintained by a DoD Component, to carry out its functions, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute

4See footnote 2 to this Appendix B.