Print Form Submit by Email

Privacy Act Self-Inspection Survey For use by those DoD IG activities following DoD IG Instruction 5400.11 (Privacy Act Program)

Requirement: DoD Directive 5400.11, DoD Privacy Program, requires the Defense Components to ensure that local Privacy Act programs are periodically reviewed by Inspectors General or other officials. The purpose of these reviews is to ensure compliance with 5 U.S.C. 552a and implementing Office of Management and Budget, and DoD guidance as well as any DoD IG-issued guidelines and procedures. While this self-inspection survey is designed to satisfy this requirement, DoD IG activities may still be subject to review by the DoD IG Privacy Office, the Defense Privacy Office, or other Federal agencies with Privacy Act oversight.

Instructions:

1. Answer each question as it is posed. Some questions are hypothetical asking what you would do if something occurred. If the situation has never occurred, do not merely state that fact. Instead, answer what you WOULD do.

2. For answers that require explanations, include them at the end of this survey or on a separate sheet, referencing the question number.

3. Be prepared to provide documentation to support any responses should that be requested by this office, DoD, or the Office of Management and Budget on any follow-up.

Completed Surveys: Email completed surveys to privacy@dodig.mil or mail hardcopies to:

DoD IG Privacy Office
400 Army Navy Drive, Suite 1034
Arlington, VA 22202-4704

This Self Inspection Module Covers 75 Questions, as follows:

Section 1: Publication Requirements - 3 Questions.
Section 2: Recordkeeping Practices - 7 Questions.
Section 3. Record Access/Amendment. - 5 Questions.
Section 4. Security of Automated Systems - 12 Questions.
Section 5. Physical Safeguards for Electronic & Manual Privacy Records - 4 Questions.
Section 6. Third Party Disclosures - 6 Questions.
Section 7. Contractor Access - 7 Questions.
Section 8. Data Collection Practices - 8 Questions.
Section 9. Computer Matching - 6 Questions.
Section 10. System of Records Exemptions - 7 Questions.
Section 11. Privacy Act Training - 5 Questions.
Section 12. Program Effectiveness - 3 Questions.

Privacy Act Self-Inspection Survey

Section I. Publication Requirements.

1a. For each Privacy Act system of records you operate, has DoD or the "owning" Federal agency issued a Federal Register notice advising the public of the existence of the system? Note: The DoD IG Privacy Act systems are available at http://www.defenselink.mil/privacy/notices/oig/. The Government-Wide Privacy Act systems are available at http://www.defenselink.mil/privacy/govwide/

- ☐ Yes.
- ☐ No.
- ☐ Don't know.

1b. During the current or prior year, did you review these Federal Register notices to ensure they were accurate for your purposes?

- ☐ Yes.
- ☐ Most were reviewed but not all (explain below).
- ☐ A few were reviewed (explain below).
- ☐ None were reviewed (explain below).

Explanation

1c. Consider the most recent occurrence, if any, when your activity wanted to use personal information in a system of records for a new routine use. Did you ask the DoD IG Privacy Office to give the public an opportunity to comment on the proposed new routine use before it went into effect?

- ☐ Yes. A Federal Register notice was issued at least 30 days before the routine use first went into effect.

  If "Yes" enter the Federal Register notice citation:
- ☐ No. (Explain below.)
- ☐ Not applicable. No routine uses were added.

Section 2. Recordkeeping Practices.

2a. When you make disclosures of data to non DoD individuals, do you maintain an accounting of those disclosures?

- ☐ Yes.
- ☐ Partial accounting. (Explain below.)
- ☐ No. Skip to question 2e.
- ☐ I don't know. Skip to question 2e.

Explanation

2b. How is the disclosure accounting maintained?
(Check all that apply.)

- ☐ For some or all systems, we maintain an up-to-date record of disclosures as they are made.
- ☐ For some or all systems, we create a retrospective record only when requested by an individual or required fro other purposes.
- ☐ Other. (Explain below.)

Explanation

2c. For disclosure accountings that are recorded as they occur, do you retain the list of disclosures for 5 years or the life of the record, whichever is greater?

- ☐ Yes.
- ☐ No.
- ☐ I don't know.
- ☐ Not Applicable. We create a retrospective record as required.

2d. If you create a retrospective record when a need arises, are you able to retrieve all disclosures made for the past 5 years or the life of the record, whichever is greater?

- ☐ Yes. Our system has that capability.
- ☐ No. (Explain below.)
- ☐ I don't know.
- ☐ Not applicable. We record the disclosure as it occurs.

Explanation

2e. When an individual's records are disclosed pursuant to a compulsory process (e.g., a court order) and that process becomes a matter of public record, does your activity take reasonable efforts to notify the subject individual that their records are being disclosed?

- ☐ Yes. (Briefly explain below.)
- ☐ No. (Briefly explain below.)

Explanation

2f. For locally devised forms, survey, questionnaires or similar documents that solicit personal information, do you have local procedures in place to ensure that they are reviewed by your local Privacy Act official before they are approved and Privacy Act Statements are added where appropriate?

- ☐ Yes. Forms and survey developers are aware of this requirement.
- ☐ No. (Briefly explain below.)
- ☐ We use no locally devised forms, surveys, questionnaires--only those generated by DoD (or DoD components) or other federal agencies.

Explanation

2g. For those employees who are required to handle Privacy Act data, do they have ready access to the governing Privacy Act system notice?

- ☐ Yes.
- ☐ No.
- ☐ I don't know.

Section 3. Record Access/Amendment. The following questions pertain to requests filed by the record subject (or his authorized agent) for access to his own file.

3a. What steps do you take to verify requester's identity before disclosing or amending records?

- ☐ For personal visits, individuals must show photo identification.
- ☐ For written requests, individuals are given a choice of having their requests notarized or providing self-sworn identity declaration statements.
- ☐ Identity is not verified. (Explain below.)

Explanation

3b. What is your estimated response time to a first party Privacy Act request for access?

- ☐ We normally respond within 20 days. (Skip to question 3d.)
- ☐ We rarely or never respond within 20 days. (Continue with question 3c.)

3c. What are the typical causes for delay in responding to Privacy Act requests? Check all that apply.

- ☐ Insufficient manpower.
- ☐ Complexity of requests.
- ☐ Difficulty extracting data from electronic systems.
- ☐ Other. (Explain below.)

Explanation

3d. If, while processing a first party Privacy Act request for access to data in a nonexempt system, you discover that third party data is contained within the individual's record or file. How would you treat that data?

- ☐ Delete it under the Personal Privacy exemption of the Freedom of Information Act (5 U.S.C. 552(b)(6)) and provide the right of appeal.
- ☐ Disclose it to the record subject since the system has not been exempted from the Privacy Act.
- ☐ I don't know.

3e. Have you ever charged a person a fee for gaining access to his own record?

- ☐ Yes. (Explain below the circumstances or type of circumstances that would cause you to charge a fee.)
- ☐ No.

Explanation

Section 4. Security of Automated Systems.

4a. Do you maintain Privacy Act records in electronic format?

- ☐ Yes.
- ☐ No. All of our records are in paper form. (Skip to Section 5.)

4b. For each database your activity operates, have those databases been placed on a Local Area Network (LAN) accredited and certified according to DoD 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) or the newer DoD Information Assurance Certification and Accreditation Process (DIACAP)?

- ☐ Yes, all of our files are on a DITSCAP or DIACAP certified LAN.
- ☐ No. Some of our files are on a certified LAN and some are on a standalone computer. (Skip to question 4d.)
- ☐ No. (Explain below.) (Skip to question 4d.)
- ☐ I don't know.

Explanation

4c. If you responded "yes" to Question 4a above for a DITSCAP, would you be able to produce a Systems Security Authorization Agreement if required?

- ☐ Yes. (Skip to section 6.)
- ☐ No. (Explain below.)
- ☐ I don't know.

Explanation

4d. If you responded "no" to in Question 4a above, do you or your IT staff monitor the management and operation of the standalone system to ensure an acceptable level of residual risk is preserved?

- ☐ Yes.
- ☐ No. (Explain below.)
- ☐ I don't know.

Explanation

4e. For each database you maintain on a standalone system, do you or your IT staff periodically assess the threats, vulnerabilities and effectiveness of current or proposed safeguards for these automated information systems?

- ☐ Yes. All systems are periodically assessed.
- ☐ No. (Explain below.)
- ☐ I don't know.

Explanation

4f. Does your activity have the means to detect when persons without authorization are reading, altering, disclosing, or destroying information stored on your standalone system?

- ☐ Yes.
- ☐ No.
- ☐ I don't know.

4g. Within the past 12 months, did any person without authorization read, alter, disclose, or destroy any personal information from one of your automated information systems (to include e-mails)?

- ☐ Yes.
- ☐ No. (Skip to question 4l.)
- ☐ I don't know. (Skip to question 4l).

4h. How many times did this occur? Enter number; if none, enter a zero. ☐

4i. How many of these times involved inappropriate access by one or more employees of your agency? (Enter number; if none, enter a zero.)

Enter number; if none, enter a zero. ☐

4j. How did your agency learn of these occurrences? (Check all that apply.)

- ☐ Audit Reports
- ☐ Received leaked/breached information
- ☐ Management oversight
- ☐ Word of mouth
- ☐ Destruction of computer file(s)
- ☐ Denial of services
- ☐ Information leaked to public domain
- ☐ Agency or activity sued in court, (Provide case styling) ☐
- ☐ Other. (Please specify. However, do not discuss in such detail that your security measures or countermeasures could or would be compromised.

Explanation ☐

4k. For the most recent such occurrence involving personal information, please briefly describe the incident, the primary reason for its occurrence, and what has been done to prevent its recurrence. (Note: Do not discuss in such detail that your security measures or countermeasures could or would be compromised.)

☐

4l. If a destructive data breach occurs, do you have a means to restore all or most of the lost data?

- ☐ Yes. The data is periodically downloaded and stored at an offsite location.
- ☐ Yes, but not by offsite storage. (Explain below.)
- ☐ No. (Explain below.)
- ☐ I don't know.

Explanation

Section 5. Physical Safeguards for Electronic and Manual Privacy Act Records.

5a. Are your paper records (including computer printouts) marked to identify them as sensitive?

- ☐ Yes - All or nearly all are marked with either the "For Official Use Only" or the "Personal Data - Privacy Act of 1974" handling legend.
- ☐ Many are marked but not all. (Explain below.)
- ☐ None or nearly none are marked. (Explain below.)
- ☐ I don't know.

Explanation

5b. Have you marked your tape or film canisters, file folders, or other housing devices to show that they contain Privacy Act data?

- ☐ Yes. All or nearly all been marked with component warning labels or other warning labels.
- ☐ Many are marked but not all. (Explain below.)
- ☐ None or nearly none are marked. (Explain below.)
- ☐ I don't know.

Explanation

5c. Has the workforce been advised that when paper records containing Privacy Act data are handcarried or transported, the contents are to be shielded from view?

- ☐ Yes. Employees have been informed to use DD Form 2923 (Privacy Act Data Sheet) or to otherwise shield the data from view.
- ☐ No. This requirement is rarely or never met. (Explain below.)
- ☐ I don't know.

Explanation

5d. Describe how you destroy Privacy Act data when it has served its intended purpose.

- ☐ Electronic data is degaussed, deleted, or overwritten.
- ☐ Paper records are shredded or treated to render them unreadable or difficult to reconstruct. This is performed by either my activity or under contract.
- ☐ Other method. (Explain below.)

Explanation

Section 6. Authorized Third Party Disclosures.

6a. Before disclosing records to an authorized nonfederal data recipient for official government purposes, how does your activity ensure the information is complete, accurate, relevant and timely? (Check all that apply.)

- ☐ We do not assure completeness, accuracy, relevance or timeliness.
- ☐ Verify with other records within agency.
- ☐ Verify with other federal agencies' records.
- ☐ Verify with the record subject.
- ☐ Verify with state and local agencies.
- ☐ Comparison with private sector records (e.g., banks, former employer).
- ☐ Our systems of records are exempt from this requirement.
- ☐ Other (Please specify.)

6b. When Privacy Act data is disclosed to an authorized nonfederal government entity, which of the following security protections does your activity impose on these non-federal government organizations? (Check all that apply.)

- ☐ They cannot provide it to other organizations.
- ☐ They must have their employees sign a statement asserting their security responsibilities.
- ☐ They must delete or return the information when it is no longer needed.
- ☐ They cannot allow any unauthorized persons to see the information.
- ☐ They must keep the records in a secure place.
- ☐ They must be penalized for not having security protections in place.
- ☐ Other (Please specify.)
- ☐ No security protections are imposed.

6c. Should another component or DoD employee (other than employees charged with responsibility for routinely maintaining or monitoring the data) ask for access to your data, what steps are taken in evaluating whether to provide the data?

- ☐ We ask why they need the data and how they intend to use it to ensure their intended use satisfies the Privacy Act subsection B requirements.
- ☐ No evaluation is conducted. We provide the data upon request.
- ☐ No evaluation is conducted. The request is automatically refused.
- ☐ Other. (Explain below.)

Explanation

6d. When a decision is made to provide data to another component or DoD employee in the situations discussed in 6c above, what restrictions are placed on the data at the time it is delivered? (Mark all that apply.)

- ☐ A warning (verbal or written) that the data is subject to the Privacy Act.
- ☐ The data may only be used for the agreed purpose.
- ☐ The data must be destroyed or returned at termination of the project.
- ☐ The data must be safeguarded during and after duty hours.
- ☐ The data may not be further disclosed.
- ☐ Other. (Explain below.)
- ☐ No restrictions or warnings are provided.

Explanation

6e. When a non-DoD organization asks for access to Privacy Act data and you have no written permission from the subject to disclose, what steps do you take in determining whether to supply the data? (Check all that apply.)

- ☐ We check Section B of the Privacy Act to see if disclosure is authorized.
- ☐ We check the "Routine Use" clause of the governing system notice to see if disclosure is authorized.
- ☐ We check the "Blanket Routine Uses," to see if disclosure is authorized.
- ☐ We contact the record subject and ask their permission to disclose.
- ☐ Our decision to disclose is based solely on the requesting agency's justification for access to the data.
- ☐ We automatically supply the data without review or evaluation.
- ☐ These requests are always routinely refused without review or evaluation.

6f. When you receive a Freedom of Information Act request from a member of the public for access to Privacy Act data, do you limit release to those data elements authorized for release by the Office of Personnel Management (OPM) in their formal rules published at 5 CFR 293.311? (Check all that apply.)

- ☐ Yes, we release only those data elements.
- ☐ Yes, we also apply the OPM standards to military personnel, releasing only those authorized data elements.
- ☐ In addition to the OPM list of releasable items, we also release education and training, including special skills, licenses, or certifications as recommended by DoD and the Department of Justice.
- ☐ To comply with 10 U.S.C.130b, we release no data about military or civilian employees stationed overseas, assigned to sensitive or routinely deployable units.
- ☐ Where applicable, to comply with 10 U.S.C. 424, we release no data about military or civilian employees assigned to the Defense Intelligence Agency, the National Reconnaissance Organization, or the National Imagery and Mapping Agency. (National Geospatial Intelligence Agency).
- ☐ We comply with the DoD policy on nondisclosure of lists of Defense personnel.
- ☐ No. My activity does not follow the OPM and/or the DoD rules for release. (Describe the data elements your activity does release in response to a FOIA requests.)

Explanation

Section 7. Contractor Access.

7a. Have you contracted out any function that would give contractors access to Privacy Act Data?

- ☐ Yes. (Continue.)
- ☐ No. Go to Section 8.

7b. For the contracts your activity awarded, do they contain FAR clauses 52.224-1 and 52.224-2 addressing Privacy?

- ☐ Yes.
- ☐ No. (Explain why).
- ☐ I don't know.

Explanation

7c. Do you have language in each contract that prohibits secondary uses of the data? (By "secondary," we are referring to any use not in direct support of the contract.)

- ☐ Yes.
- ☐ No. (Explain below.)

Explanation

7d. Do the contractor employees have access to the appropriate system of records notices and DoD IG (or DoD) Privacy Act regulations?

- ☐ Yes.
- ☐ No. (Explain below.)
- ☐ I don't know.

Explanation

7e. Do your current contracts address disposition of the data at the end of the contract?

- ☐ Yes.
- ☐ No. (Explain below.)
- ☐ I don't know.

Explanation

7f. During the past 2 years, did your activity review the performance of the contractor to ensure it was complying with the Privacy Act?

☐ Yes.

☐ No. (Please briefly explain.)

Explanation

7g. If you answered "yes" to Q7f, provide a brief description of what your review consisted

Explanation

Section 8. Data Collection Practices.

8a. For individuals who are asked to supply personal information on forms, surveys, questionnaires, or other formats, does your agency inform them, in writing, of: (Check one for each statement.)

8a-1. The authority for requesting the information? (Check one.)

☐ Yes.

☐ No. (Please briefly explain.)

Explanation

8a-2. How the information may be used? (Check one.)

☐ Yes.

☐ No. (Please briefly explain.)

Explanation

8a-3. Whether providing the information is mandatory or voluntary? (Check one.)

☐ Yes.

☐ No. (Please briefly explain.)

Explanation

8a-4. The consequences of not providing the information? (Check one.)

☐ Yes.

☐ No. (Please briefly explain.)

Explanation

8a-5. The governing system notice that applies to the collection.

☐ Yes.

☐ No. (Please briefly explain.)

Explanation

8b. Do you maintain Internet or Intranet websites that require visitors to the site to enter their SSN, birth date, or other personal data to gain access to the site?

☐ Yes.

☐ No. (Go to Question 8e.)

Explanation

8c. If you answered "yes" to Q8b, provide your website URL's and the data elements you collect at each site.

Web Site Address (URL)	Data Elements Collected

8d. If your website collects SSN, does your site include a Privacy Act Statement at the entrance to the site advising the visitor of your authority for collecting SSN, the purpose what uses will be made of it, and whether providing SSN is mandatory or voluntary to gain access to the database.

- ☐ Yes, all that information is supplied at the site.
- ☐ No. (Explain below.)

Explanation

8e. For your Internet or Intranet websites, do you employ computer cookies to track visitors? (Check all that apply.)

- ☐ Yes, we use session cookies that expires when the visitor closes his browser or exits the site. (Go to Question 8g.)
- ☐ Yes, we use persistent cookies that remain on the visitor's hard drive. (Continue.)
- ☐ We use no cookies. (Go to Question 8g.)

8f. If you answered "Yes" to persistent cookie use, did you receive written approval for the use of the persistent cookie from the appropriate authority?

- ☐ Yes. The Secretary of Defense approved the use of a persistent cookie.
- ☐ No. (Explain below.)
- ☐ I don't know.

Explanation

8g. Assume that the head of your activity or other management official has directed that you immediately set up a new system to collect personal data on individuals. Since time is of the essence, he gives you a two week deadline to get the system established and to populate the database. What is your **foremost** concern in responding to this tasking? Select only one.

- ☐ Meeting the deadline.
- ☐ Complying with Privacy Act requirements.
- ☐ Meeting the deadline while doing your best to comply with the Privacy Act requirements.

8h. What steps would you take in responding to the tasking in Question 8g? Check all that apply.

- ☐ Consult with Privacy officials.
- ☐ Gather material for or assist in drafting a system notice for publication in the Federal Register.
- ☐ Work with Information Technology staff to begin creating the database framework and readying it for future launch.
- ☐ Work with Records Management officials to ensure that disposition rules are approved for the new data collection.
- ☐ Work with Information Technology officials to limit access to the data to those employees who need the data to perform assigned duties.
- ☐ Notify the head of your activity or other management official that complying with Privacy Act requirements may delay the actual launch of the database.
- ☐ Verify the need for collectiing and storing the personal data.
- ☐ Other. (Explain below.)

Section 9. Computer Matching.

9a. Are your Privacy Act records used in any computer matching program? (Check one.)

- ☐ Yes. (Continue.)
- ☐ No. (Go to Section 10.)

9b. Are your records used solely to conduct computer matches with records of your own Component?

- ☐ Yes. (Go to Section 10.)
- ☐ No. We conducted matches with other DoD Components or other Federal agencies or non-Federal entities. (Continue.)

9c. If your matches are solely with other DoD Components, do you routinely notify the Defense Privacy Office before conducting such matches?

☐ Yes, in all cases. (Go to Section 10.)

☐ No. (Please explain.) (Go to Section 10.)

Explanation

Note: Questions 9d through 9f pertain to matches conducted with another Federal agency or another non-Federal entity.

9d. During the past year, did your activity review the matching programs to ensure that the requirements of the Privacy Act and OMB guidance were met? (Check one.)

☐ Yes.

☐ Some. (Please briefly explain.)

☐ No. (Please briefly explain.)

Explanation

9e. Are your matching programs approved by the Defense Data Integrity Board? (Check one.)

☐ Yes.

☐ No. (Please briefly explain.)

Explanation

9f. Should a case occur where you act as the source agency and a State or local government is the recipient agency, who publishes the notice of the match in the Federal Register?

- ☐ We do since State and local governments do not have Federal Register publishing rights.
- ☐ The State or local government since they are the recipient agency.
- ☐ I don't know.

Section 10. System of Records Exemptions.

10a. Do you maintain any DoD IG, DoD wide or government wide Privacy Act systems of records that are exempt from any provision of the Privacy Act? (Check one.)

- ☐ Yes. (Continue.)
- ☐ No. (Go to Section 11.)
- ☐ I don't know. (Go to Section 11.)

10b. List the names of the Privacy Act systems along with the DoD IG, DoD wide or government wide system designators. A list of DoD IG and DoD wide systems (and used government wide systems in DoD IG) is published at http://www.defenselink.mil/privacy/.

List of Names

10c. Before responding to a first-party Privacy Act request, do you routinely check the system notice to see if the files have been exempted from the requirement to allow access?

- ☐ Yes, in all instances.
- ☐ No. I am aware of which systems are exempt and which exemptions are claimed.
- ☐ No. Other. (Explain.)

Explanation

10d. After determining that a Privacy Act exemption applies, do you consider the exempt portions for release under the Freedom of Information Act?

- ☐ Yes, in all instances.
- ☐ No.

10e. Before issuing a Privacy Act full or partial denial, do you ask your Office of General Counsel to review and coordinate on your proposed response?

- ☐ Yes, in all instances.
- ☐ No.

10f. When issuing a first party Privacy Act full or partial denial, do you cite both the Privacy and the FOIA exemptions in your response letter?

- ☐ Yes, in all instances.
- ☐ No.

10g. When issuing a first party Privacy Act access denial (full or partial), do you include the right of appeal in your response?

- ☐ Yes, in all instances.
- ☐ No. The Privacy Act contains no right of appeal for access denials.
- ☐ No. (Other reason.) Explain.

Explanation

Section 11. Privacy Act Training.

11a. Consider all persons with access to the personally identifiable information in your systems of records. About what portion of these persons have been adequately trained in the Privacy Act? (Check one.)

- ☐ All or almost all.
- ☐ More than half.
- ☐ About half.
- ☐ Less than half.
- ☐ None or almost none

11b. For individuals who have received Privacy Act training, what was the source of that training? Check all that apply.

- ☐ Annual and/or specialized Privacy Training.
- ☐ Formal training from Federal agencies (e.g., USDA Grad School, OPM.)
- ☐ Formal training from schools or universities.
- ☐ Formal training from societies (e.g. ASAP).
- ☐ DoD or DoD IG Privacy Office administered training programs.
- ☐ Training programs administered by local Privacy Act officials.
- ☐ Independent reading of DoD/DoD IG Privacy Act regulations.
- ☐ Other. (Explain.)

Explanation

11c. For individuals who have received little or no Privacy Act training, what do you believe is the primary cause? (Check all that apply.)

- ☐ Lack of funding.
- ☐ Lack of time to devote to training.
- ☐ Unaware of the requirement.
- ☐ Privacy training is overshadowed by other needs.
- ☐ Unaware of training sources.
- ☐ Other. (Explain.)

Explanation

11d. Does your local director or other management official periodically cover Privacy Act procedures or issue Privacy Act reminders in staff meetings, calls, town or similar events?

- ☐ Yes.
- ☐ No.

11e. Do new employees receive indoctrination training on Privacy Act or For Official Use only procedures and penalties for misuse of internal data?

- ☐ Yes.
- ☐ No.

Section 12. Program Effectiveness.

12a. Do you believe you have reasonable and timely access to:

12a-1: Legal advice?

- ☐ Yes.
- ☐ No. (Please explain.)

12a-2. Advice on administrative or procedural matters?

- ☐ Yes.
- ☐ No. (Please explain.)

12a-3. Formal rules, guidelines, or other written Privacy Act material?

- ☐ Yes.
- ☐ No. (Explain below.)

12b. Do you have recommendations for making the DoD IG Privacy Act program more effective?

- ☐ Yes. (List below.)
- ☐ No.

Recommendations

12c. Do you have any Privacy Act concerns that were not addressed on this self-inspection survey?

☐ Yes. (list below)

☐ No.

Concerns

Name:

Contact Phone Number:

Email Address:

Name of DoD IG Component:

Privacy Official Contact (POC):
(if different than above)

End of Survey.
Thank you for completing this mandatory requirement.