INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

January 14, 2020

INSPECTOR GENERAL INSTRUCTION 5400.11

PRIVACY PROGRAM

FOREWORD

This instruction provides guidance and procedures for implementing the Privacy Program within the DoD Office of Inspector General.

This instruction will expire 10 years from its issuance date.

The office of primary responsibility for this instruction is the Office of General Counsel. This instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

Steven A. Stebbins
Chief of Staff

4 Appendices

PRIVACY PROGRAM

TABLE OF CONTENTS

Paragraph **Page**

CHAPTER 1
GENERAL

A. Purpose 3
B. Cancellation 3
C. Summary of Changes 3
D. Applicability 3
E. References 3
F. Definitions 3
G. Acronyms and Abbreviations 3
H. Policy 3
I. Responsibilities 3

CHAPTER 2
PROCEDURES

A. Publication of Notice in the Federal Register 9
B. Access to Systems of Records Information 9
C. Access to Records or Information in Exempt Systems 9
D. Requesting Changes to Personal Information in Systems of Records 10
E. Amending Personal Information in Systems of Records 10
F. Denying Amendments to Personal Information in Systems of Records 10
G. Records Controlled and Maintained by Another Agency 11
H. Filing an Appeal 11
I. Processing Appeals 11
J. Disclosure of Disputed Information 11
K. Penalties 12
L. Computer Matching Programs 12
M. Breach Response 12

APPENDICES

A. References 14
B. Definitions 16
C. Acronyms and Abbreviations 18
D. Breach Reporting Requirements 19

CHAPTER 1
GENERAL

A. Purpose. This instruction provides the DoD Office of Inspector General (OIG) with guidance and procedures for implementing the Privacy Program according to references (a) through (d).

B. Cancellation. This instruction cancels IG Instruction 5400.11, *Privacy Act Program*, January 29, 2010.

C. Summary of Changes. This revision includes minor changes, such as office names and updated references. It also further defines the responsibilities of senior-level officials and Components in the administration of the Privacy Program because of a change in organizational structure. This instruction incorporates specific procedures to follow in the event of a known or suspected breach and creates a training requirement for all employees that regularly work with records containing personally identifiable information (PII).

D. Applicability. This instruction applies to the OIG.

E. References. (See Appendix A.)

F. Definitions. (See Appendix B.)

G. Acronyms and Abbreviations. (See Appendix C.)

H. Policy. It is OIG policy that all PII collected, maintained, and used by the OIG will be safeguarded and handled according to references (d) and (e).

I. Responsibilities.

1. The **Senior Component Official for Privacy (SCOP)** will:

a. Direct and administer the DoD Privacy Program for the OIG.

b. Serve as the appellate authority for the OIG when a requester appeals a denial of access to, or an amendment of, a record.

c. Establish standards and procedures to ensure implementation of and compliance with references (b) and (c).

d. Provide advice and assistance to senior officials on matters pertaining to reference (d).

e. Review and approve all System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), and Social Security number (SSN) Justification Memorandums according to references (b), (c), and (d).

f. Serve as a member of the Defense Data Integrity Board according to reference (b).

g. Ensure completion of required reports to the Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD), the DoD Chief Management Officer (CMO), the Office of Management and Budget (OMB), and other required organizations, including:

(1) The annual Federal Information Security Management Act report to the DPCLTD according to reference (f);

(2) The semi-annual Component Privacy and Civil Liberties report to the DoD CMO according to reference (g);

(3) The Social Security Fraud Prevention Act of 2017 report to the DPCLTD according to reference (h);

(4) Civil liberties violations and their dispositions to the DPCLTD according to reference (b); and

(5) Other reports, as required.

h. Manage all breaches in the agency with the support of the Freedom of Information Act (FOIA), Privacy and Civil Liberties Office and the Breach Response Team (BRT).

i. Ensure that the required breach reporting occurs within statutory deadlines, including reporting to the DPCLTD and the U.S. Computer Emergency Readiness Team (US-CERT) according to reference (f) and Appendix D.

j. Coordinate, as appropriate, with the DoD Senior Agency Official for Privacy and the DoD Office of General Counsel (OGC) to determine if a “major” breach has occurred according to references (i) and (j).

k. Conduct an assessment of the risk of harm to individuals potentially affected by a breach according to references (j) and (k).

l. Determine how to best mitigate the harm to individuals affected by a breach according to reference (j).

m. Determine whether to notify affected individuals of the breach according to reference (j).

n. Determine and initiate actions in response to a breach, including countermeasures, acquisition of additional staff, resources, or services to offer individuals affected or potentially affected by a breach according to reference (j).

2. The **Component Heads** will:

a. Designate an individual as the Component point of contact (POC) for privacy matters and advise the FOIA, Privacy and Civil Liberties Office of the POC's name and contact information. The POC should have a thorough understanding of the Component's record-keeping systems and processes.

b. Forward all requests for access to records to the FOIA, Privacy and Civil Liberties Office for processing.

c. Provide requested records without redactions to the FOIA, Privacy and Civil Liberties Office within the requested timeframe.

d. Provide justification to the FOIA, Privacy and Civil Liberties Office when the Component recommends denial of access to a record in whole or in part.

e. Amend records when they are no longer accurate, relevant, timely, or complete.

f. Report any new record system, or changes to an existing system, to the FOIA, Privacy and Civil Liberties Office at least 90 days before the intended use of the system.

g. Provide responses in the requested timeframe to the FOIA, Privacy and Civil Liberties Office regarding reviews of each SORN on a biennial basis and as requested.

h. Include appropriate Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement clauses in all contracts where contractor personnel are required to access records systems covered by the Privacy Act.

i. Conduct risk assessments and coordinate with the FOIA, Privacy and Civil Liberties Office prior to initiating any new activities that involve the creation, collection, use, process, storage, maintenance, dissemination, disclosure, or disposal of PII, and ensure that appropriate PIA, SORN, Privacy Act statement, and other requirements are met prior to initiating new collections.

j. Report any known or suspected breaches, as soon as they are identified, to the FOIA, Privacy and Civil Liberties Office, Office of the Chief Information Officer, and other appropriate entities according to Appendix D.

k. Take necessary actions to mitigate a known breach and prevent reoccurrence in coordination with the SCOP and the FOIA, Privacy and Civil Liberties Office.

l. Investigate the cause of a breach and provide the FOIA, Privacy and Civil Liberties Office with the required information according to Appendix D.

m. Submit an "After Action Report" to the Chief Information Officer (CIO), FOIA Privacy and Civil Liberties Office, and SCOP within 30 days of breach discovery.

n. Include a Privacy Act statement on all forms that collect sensitive PII from individuals.

o. Ensure that all record disclosures from a Privacy Act system of records are not disclosed outside the DoD without a corresponding routine use published in the Federal Register.

p. Maintain a log of all releases of PII to outside agencies.

q. Ensure that all Component employees who handle, or have access to, PII as a regular part of their official duties complete annual training.

3. The **FOIA, Privacy and Civil Liberties Office** will:

a. Provide appropriate guidance according to reference (d).

b. Provide appropriate privacy training for all onboarding personnel, and specialized privacy training when deemed necessary by Components.

c. Compile data from the Components and submit required reports to the DPCLTD, DoD CMO, OMB, and other required organizations.

d. Review and maintain PIAs and SORNs according to references (d) and (l).

e. Review all proposed OIG or Component-level forms that collect PII according to references (b) and (c).

f. Review OIG-wide policies or other methods used to collect information about individuals to ensure compliance with reference (c).

g. Report known or suspected breaches to the DPCLTD according to reference (c), and assist affected Components in their breach response duties according to Appendix D.

h. Complete required breach reporting to the SCOP, US-CERT, DPCLTD, and other required entities according to reference (c) and Appendix D.

i. Serve as a liaison between Components and the SCOP.

j. Provide the SCOP with the PIAs, SORNs, and privacy notices applicable to compromised information.

k. Document and report all breaches and actions taken in response to a breach using the DD Form 2959, *Breach of Personally Identifiable Information (PII) Report*, and submit the form to the DPCLTD.

l. Coordinate or provide notification to the public and affected individuals, if deemed necessary.

4. The **CIO** will:

a. Analyze and document privacy risks when considering information technology (IT) investments in proposed systems or modifications to existing systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

b. Develop privacy controls and a continuous monitoring strategy to manage risk according to references (e), (m), and (n).

c. Serve as the principal IT/cybersecurity POC for all breaches and when necessary, appoint a representative to the BRT according to Chapter 2, paragraph M.3.

d. Evaluate the effectiveness of information security measures in place to protect against PII breaches.

e. Work with affected Components to determine the likelihood and extent of a breach, to include the data sets compromised and the number of individuals affected.

f. Evaluate the effectiveness of information security mitigating actions.

g. Determine if forensics support services should be obtained when a breach involves the suspected or actual infiltration of an IT system for malicious purposes.

h. Serve as the lead for "After Action Reports" for breaches that occur because of security infiltration, programmatic error, or other technical factors independent of human error.

i. Provide technical data to support breach response reporting, when necessary.

5. The **Chief of Staff (CoS)** will coordinate any breach response activities requiring the use of Mission Support Team staff from more than one MST Directorate and may delegate to the Deputy Chief of Staff (DCoS).

6. A **Requester** will be required to:

a. Submit a written request for access to records that pertain to themselves to the FOIA, Privacy and Civil Liberties Office.

b. Provide proof of identity in the form of an unsworn declaration or notarized request.

c. Describe the records sought and provide sufficient information to enable the requested records to be located, such as the name of the system of records, approximate date the record was created, originating organization, or type of document.

d. Submit a written request to amend a record to the FOIA, Privacy and Civil Liberties Office.

CHAPTER 2
PROCEDURES

A. Publication of Notice in the Federal Register.

1. All SORNs must be published in the Federal Register prior to system use.

2. The Component Heads will submit SORNs for new or revised systems of records to the FOIA, Privacy and Civil Liberties Office at least 90 days prior to implementation.

3. The FOIA, Privacy and Civil Liberties Office will review and forward complete SORNs to the DPCLTD for review and publication in the Federal Register.

B. Access to Systems of Records Information.

1. Individuals may request access to their records by mail or electronically according to the following procedures:

a. An individual submitting a request may use the FOIA request portal or send in a request to the Department of Defense, Office of Inspector General, FOIA, Privacy and Civil Liberties Office, 4800 Mark Center Drive, Suite 10B24, Alexandria, VA 22350-1500.

b. For verification purposes, a request will contain a signed, notarized statement or a signed unsworn declaration made under penalty of perjury according to reference (o). Individuals may select the declaration in the FOIA request portal.

2. The requester does not need to state a reason or justify the need to gain access to records.

3. No verification of identity will be required of an individual seeking access to records that are available to the public.

4. According to reference (d), requesters will not be denied access to their records for refusing to disclose their SSN, unless disclosure of the SSN is required by statute or by regulation adopted before January 1, 1975.

C. Access to Records or Information in Exempt Systems. The FOIA, Privacy and Civil Liberties Office processes requests to give requesters a greater degree of access to records on themselves.

1. Records, including those in the custody of law enforcement activities that have been incorporated into a system of records and exempted from access, will be processed according to Chapter 3 of reference (c). When access is denied due to a claimed Privacy Act exemption, the FOIA, Privacy and Civil Liberties Office will process the request to provide information that is releasable under the FOIA.

2. The FOIA, Privacy and Civil Liberties Office will process requests for records within a system covered by the Privacy Act under both the Privacy Act and the FOIA in order to allow the maximum extent of disclosure to a first party requester.

3. Exempt records temporarily in the custody of another Component are considered the property of the originating Component. Access to these records is controlled by the system notices and rules of the originating Component.

D. Requesting Changes to Personal Information in Systems of Records. Individuals may request amendment of their records when such records are believed to be inaccurate, irrelevant, untimely, or incomplete.

1. Requests to amend records must be sent to the FOIA, Privacy and Civil Liberties Office, and must include sufficient information to locate the record, the items in the record to be amended, the reason for the amendment, appropriate justification or documentary evidence to support the requested amendment, and the type of action sought, such as deletion, correction, or addition.

2. The FOIA, Privacy and Civil Liberties Office coordinates the processing of the amendment request with the Component.

3. Requesters are required to provide verification of their identity to ensure that they are seeking to amend records about themselves and not the records of others.

4. The FOIA, Privacy and Civil Liberties Office will mail written acknowledgment of an individual's request to amend a record within 10 working days of receipt.

E. Amending Personal Information in Systems of Records. The Component decides whether to grant an amendment to the records. If the Component grants all or any portion of an individual's request to amend a record, the Component will:

1. Amend the record according to reference (d).

2. Inform the FOIA, Privacy and Civil Liberties Office of the action taken and provide a copy of the corrected record for release to the requester. The FOIA, Privacy and Civil Liberties Office will respond to the requester on behalf of the OIG.

3. Notify all previous holders known to be retaining the record of information that the amendment has been made and explain the substance of the correction.

F. Denying Amendments to Personal Information in Systems of Records.

1. A Component may deny an amendment request if the information in the record is accurate, timely, relevant and complete.

2. The Component will provide a copy of the justification for denial to the FOIA, Privacy and Civil Liberties Office if the Component denies all or any portion of a request.

3. The FOIA, Privacy and Civil Liberties Office may request a Component to clarify or explain any justification for denial.

4. The FOIA, Privacy and Civil Liberties Office will advise the requester of the reason for the denial and provide them with appeal rights.

G. Records Controlled and Maintained by Another Agency. If the request for an amendment pertains to a record controlled and maintained by another Federal agency, the FOIA, Privacy and Civil Liberties Office will coordinate with the Component and will refer the requester to the appropriate agency.

H. Filing an Appeal. If an individual disagrees with a Component's denial determination, they may file an appeal within the OIG.

1. The appeal should be sent to the Department of Defense, Office of Inspector General, FOIA, Privacy and Civil Liberties Office, 4800 Mark Center Drive, Suite 10B24, Alexandria, VA 22350-1500.

2. The FOIA, Privacy and Civil Liberties Office will:

a. Coordinate the appeal with the SCOP and OGC. An appeal package will be developed and include: the Component's justification and authority for the denial; and comments from the FOIA, Privacy and Civil Liberties Office and OGC on the merits of the appeal.

b. Mail written acknowledgement of an individual's appeal within 10 working days of receipt.

3. If the appeal is denied, the FOIA, Privacy and Civil Liberties Office will provide the requester with the procedures for filing a statement of disagreement.

4. If the appeal is granted, the FOIA, Privacy and Civil Liberties Office will coordinate with the Component for amendment to the record and ensure compliance with Chapter 2, paragraph E.

I. Processing Appeals. The SCOP will process all appeals in a timely manner. The FOIA, Privacy and Civil Liberties Office will inform the individual, in writing, of the reasons for any delay and of the approximate date the review is expected to be completed, if a fair and equitable review cannot be made within 30 days of the receipt of the request.

J. Disclosure of Disputed Information. Following the notification of the denial of an appeal for a request for amendment, an individual may file a concise statement of disagreement of the factual content in the record. The Component will:

1. Incorporate the statement of disagreement into the record and include a brief summary of its reasons for refusing to amend the record.

2. Advise previous recipients known to be retaining the record or information that the record has been disputed and provide a copy of the individual's statement of disagreement.

3. Maintain the statement of disagreement to permit ready retrieval whenever the disputed portion of the record is disclosed.

4. Provide a copy of the individual's statement of disagreement whenever the record is disclosed to other agencies.

5. Treat the statement of disagreement as part of the individual's record and not subject it to amendment procedures.

K. Penalties.

1. Civil Action. An individual may file a civil suit against the OIG or its employees if the individual believes his or her rights under reference (d) have been violated.

2. Criminal Action. Criminal penalties may be imposed against an employee for certain offenses as follows: willfully and knowingly disclosing protected information to anyone not entitled to receive it; willfully maintaining a system of records without meeting notice requirements; or willfully and knowingly requesting or obtaining any record concerning an individual from an agency under false pretenses. An employee may be charged with a misdemeanor and fined up to $5,000 for a violation.

L. Computer Matching Programs. All requests for participation in a matching program, either as a matching agency or a source agency, will be submitted to the DPCLTD for review and compliance.

M. Breach Response. This section and Appendix D establish procedures to follow in the event of a known or suspected loss of PII, also known as a breach. Reference (p) comprises guidance for the OIG to follow in the event of a major breach, and reference (j) provides existing federal breach response requirements. The OIG must report compliance with these requirements annually according to reference (f).

1. Reference (j) defines a breach as an incident where there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where:

a. a person other than an authorized user accesses or potentially accesses PII; or

b. an authorized user accesses or potentially accesses PII for an other than authorized purpose.

2. This section applies to any breach of PII in systems maintained by the OIG, including the PII of Service members, civilian employees, contractor employees, and members of the public. It does not apply to national security systems as defined in reference (q). This section does not encompass all activities that may be required during a breach. A breach may require additional technical activities according to reference (r). Those responsibilities are outside the scope of this document.

3. A BRT will form when a complex breach is reported.

a. The SCOP will convene and lead the BRT for the OIG to review, assess, and respond to suspected or confirmed breaches of PII. The SCOP will convene the BRT within 48 hours of a confirmed or suspected breach, if deemed necessary.

b. The BRT will include critical members and situational members. Critical members participate in every breach, while situational members participate when there is a major breach, or the breach involves the respective Component's information. BRT members may designate a representative to fill their role; however, designees must possess sufficient authority on behalf of their members to permit efficient and effective BRT operations.

(1) The critical BRT members are the:

(a) SCOP;

(b) Director, FOIA, Privacy and Civil Liberties Office; and

(c) CIO.

(2) The situational team members are the:

(a) CoS or DCoS;

(b) breach-affected Component Heads;

(c) OGC;

(d) Assistant Inspector General for Legislative Affairs and Communications;

(e) Director, Office of Security; and

(f) any other OIG official identified by the SCOP.

APPENDIX A
REFERENCES

a. DoD Directive 5106.01, *Inspector General of the Department of Defense (IG DoD)*, April 20, 2012, as amended

b. DoD Instruction 5400.11, *DoD Privacy and Civil Liberties Programs*, January 29, 2019

c. DoD 5400.11-R, *Department of Defense Privacy Program*, May 14, 2007

d. Section 552a of Title 5, United States Code, *The Privacy Act of 1974*

e. Office of Management and Budget Circular No. A-130, Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources*, July 28, 2016

f. Chapter 35 of Title 44, United States Code, *Federal Information Security Modernization Act of 2014*

g. Chapter 21E of Title 42, United States Code, *Privacy and Civil Liberties Protection And Oversight*

h. Chapter 405 of Title 42, United States Code, *Evidence, procedure, and certification for payments*

i. Office of Management and Budget Memorandum M-20-04, Fiscal Year 2019-2020 *Guidance on Federal Information Security and Privacy Management Requirements*, November 19, 2019

j. Office of Management and Budget Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017

k. DoD Director of Administration and Management Memorandum, *Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations*, August 2, 2012

l. DoD Instruction 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*, July 14, 2015, as amended

m. National Institute of Standards and Technology Special Publication 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, December 18, 2014

n. Committee on National Security Systems Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 27, 2014

APPENDIX A (continued)
REFERENCES

o. Section 1746 of Title 28, United States Code, *Unsworn declarations under penalty of perjury*

p. Deputy Secretary of Defense Memorandum, *Reporting of Breaches of Personally Identifiable Information in Accordance with the Department of Defense Breach Response Plan*, November 30, 2018

q. Section 3552(b)(6) of Title 44, United States Code, *Definitions*

r. National Institute of Standards and Technology Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 8, 2012

APPENDIX B
DEFINITIONS

1. **access.** The review of a record or a copy of a record, or parts thereof, in a system of records by any individual.

2. **agency.** For the purposes of disclosing records subject to the Privacy Act among the DoD Components, the DoD is a considered a single agency. For all other purposes, to include requests for access and amendment, denial of access, or amendment, appeals from denials, and record keeping, as relating to the release of records to non-DoD Agencies, each DoD Component is considered an agency.

3. **breach.** An incident where there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. A breach is defined as major if it involves PII that, if exfiltrated, modified, deleted or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.

4. **computer matching program.** The computerized comparison of two or more automated systems of records or a system of records with non-federal records. Manual comparison of systems of records or a system of records with non-federal records are not covered.

5. **disclosure.** The transfer of any personal information from a system of records by any means of communication, such as oral, written, electronic, mechanical, or actual review to any person, private entity, or Government agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

6. **individual.** A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual may also act on behalf of an individual. Members of the U.S. Armed Forces are "individuals." Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals" when acting in an entrepreneurial capacity with the DoD, but are "individuals" when acting in a personal capacity, such as security clearances, entitlement to DoD privileges or benefits.

7. **maintain.** The term "maintain" includes maintain, collect, use or disseminate according to reference (i).

APPENDIX B (continued)
DEFINITIONS

8. **personal information.** Information about an individual that identifies, links, relates, or is unique to, or describes them, such as a SSN; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; other demographic, biometric, personnel, medical, and financial information. Such information also is known as personally identifiable information, such as information that can be used to distinguish or trace an individual's identity, such as their name; SSN; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual.

9. **record.** Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, their education, financial transactions, medical history, and criminal or employment history and that contains their name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph according to reference (i).

10. **routine use.** The disclosure of a record outside the DoD for a use that is compatible with the purpose for which the information was collected and maintained by the DoD. The routine use will be included in the published system notice for the system of records involved.

11. **source agency.** Any agency that discloses records contained in a system of records to be used in a computer-matching program, or any state or local government or agency thereof, which discloses records to be used in a computer matching program.

12. **system manager.** A Component head or designated official who has overall responsibility for a system of records. The system manager may serve at any level in the OIG. Systems managers are indicated in the published systems of records notices. If more than one official is indicated as a system manager, initial responsibility resides with the manager at the appropriate level, such as for local records, at the local activity.

13. **system of records.** A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual according to reference (i).

14. **System of Records Notice (SORN).** Statement providing to the public notice of the existence and character of a group of records under the control of any agency, from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

APPENDIX C
ACRONYMS AND ABBREVIATIONS

BRT	Breach Response Team
CIO	Chief Information Officer
CMO	Chief Management Officer
DCoS	Deputy Chief of Staff
DPCLTD	Defense Privacy, Civil Liberties, and Transparency Division
FOIA	Freedom of Information Act
IT	information technology
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	personally identifiable information
POC	point of contact
SCOP	Senior Component Official for Privacy
SORN	System of Records Notice
SSN	Social Security number
US-CERT	U.S. Computer Emergency Readiness Team

APPENDIX D
BREACH REPORTING REQUIREMENTS

The following table summarizes the time-sensitive breach reporting requirements. (See Chapter 1, paragraph I., "Responsibilities," and Chapter 2, paragraph M., "Breach Response" for other breach response requirements.

RESPONSIBLE INDIVIDUAL	TIME FRAME	ACTION REQUIRED	REFERENCES AND RESOURCES
Component Head	**Personally identifiable information breach is confirmed or suspected – Upon identification**	• **Report details of potential breach to the FOIA, Privacy and Civil Liberties Office, Office of the Chief Information Officer, and appropriate law enforcement agency (if criminal intent is indicated).** • **Identify compromised files, folders, or documents to the Office of the Chief Information Officer and the FOIA, Privacy and Civil Liberties Office; if possible, work with the Office of the Chief Information Officer to lock down compromised files, folders, or links.** • **Provide initial DD2959, *Breach of Personally Identifiable Information Report*, to the FOIA, Privacy and Civil Liberties Office.**	• **Office of Management and Budget Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017** • **National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, April 2010** • **Deputy Secretary of Defense Memorandum, *Reporting of Breaches of Personally Identifiable Information in Accordance with the Department of Defense Breach Response Plan*, November 30, 2018**
Director, FOIA, Privacy and Civil Liberties Office	**Within 1 hour**	• **Report details of breach to the United States Computer Emergency Readiness Team (US-CERT).**	• **Deputy Secretary of Defense Memorandum, *Reporting of Breaches of Personally Identifiable Information in Accordance with the Department of Defense Breach Response Plan*, November 30, 2018** • **The Federal Information Security Modernization Act of 2014**
Director, FOIA, Privacy and Civil Liberties Office and Senior Component Official for Privacy	**Within 24 hours**	• **Report details of breach to Senior Component Official for Privacy.** • **Assign tracking number.**	• **Defense Privacy, Civil Liberties, and Transparency Division Memorandum, *Requirement to File Department of Defense Breaches in the Compliance and Reporting Tool*, February 19, 2015** • ***Reporting of Breaches of Personally Identifiable Information in Accordance with the Department of Defense Breach Response Plan*, November 30, 2018**
Director, FOIA, Privacy and Civil Liberties Office and Senior Component Official for Privacy	**Within 48 hours**	• **Submit breach report to the Defense Privacy, Civil Liberties, and Transparency Division.** • **Initiate Breach Response Team (if appropriate).**	
Director, FOIA, Privacy and Civil Liberties Office and Senior Component Official for Privacy	**Within 10 days**	• **Conduct risk analysis.** • **Send notification letter to each affected individual (if directed).**	• **DoD Director of Administration and Management Memorandum, *Use of Best Judgment for Individual Personally Identifiable Information Breach Notification Determinations*, August 2, 2012**
Chief of Staff	**If required**	• **Provide identity theft protection services using government-wide blanket purchase agreement, if applicable.**	• **Office of Management and Budget Memorandum M-16-14, *Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response*, July 1, 2016**
Component Head	**Within 30 days**	• **Close out breach with "After Action Report" to the FOIA, Privacy and Civil Liberties Office.**	