DoD Manual 5400.11, Volume 2

DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan

Originating Component:	Office of the Director of Administration and Management
Effective:	May 6, 2021
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	Chapter 10, Section C10.6 and Appendix 2 of DoD 5400.11-R "Department of Defense Privacy Program," May 14, 2007 Director of Administration and Management Memorandum, "Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations," August 2, 2012 Part I, III, IV, and Appendix A of Director of Administration and Management Memorandum, "Safeguarding Against and Responding to the Breach of PII," June 5, 2009 Office of the Deputy Chief Management Officer Memorandum, "DoD Breach Response Plan," September 28, 2017
Approved by:	Thomas M. Muir, Interim Director of Administration and Management

Purpose: This manual is composed of two volumes, each containing its own purpose. In accordance with the authority in DoD Directive 5105.53, the January 11, 2021 Deputy Secretary of Defense Memorandum, and DoD Instruction (DoDI) 5400.11:

- This manual implements policy, assigns responsibilities, and provides procedures for compliance with Section 552a of Title 5, United States Code (U.S.C.), also known and referred to in this volume as the "Privacy Act of 1974," as amended, and the Office of Management and Budget (OMB) Circular No. A-130.
- This volume assigns responsibilities and provides procedures for preparing for and responding to known or suspected breaches of personally identifiable information (PII). In accordance with OMB Memorandum M-17-12, this volume serves as the DoD Breach Preparedness and Response Plan, sometimes referred to as the "Plan" in this volume.

TABLE OF CONTENTS

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This volume applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD including the DoD Intelligence Components (referred to collectively in this volume as the "DoD Components").

b. With the exception of Paragraph 6.1., this volume does not apply to national security systems as defined in Section 3552(b)(6) of Title 44, U.S.C. However, DoD Components operating national security systems are encouraged to apply this Plan to those systems if practicable. DoD Components operating systems on the SECRET Internet Protocol Router Network (SIPRNET) or the Joint Worldwide Intelligence Communications System (JWICS) must still comply with the requirements in Paragraph 6.1.

1.2. POLICY.

In accordance with DoDI 5400.11, as part of a comprehensive privacy and civil liberties program, DoD Components must comply with OMB Memorandum M-17-12 and this volume to report, respond to, and mitigate PII breaches.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR OF ADMINISTRATION AND MANAGEMENT (DA&M).

In addition to the responsibilities in Paragraph 2.8., the DA&M, in his or her capacity as DoD Privacy and Civil Liberties Officer in accordance with DoD Directive 5105.53, DoDI 5400.11, and the January 11, 2021 Deputy Secretary of Defense Memorandum:

a. Oversees the implementation and administration of this volume.

b. Advises the Secretary of Defense and senior DoD leadership on major incidents involving PII.

2.2. DIRECTOR, DIRECTORATE FOR OVERSIGHT AND COMPLIANCE (DO&C).

Under the authority, direction, and control of the DA&M, the Director, DO&C:

a. Serves as the DoD Senior Agency Official for Privacy (SAOP) responsible for leading a DoD Breach Response Team to review, assess, and respond to major incidents involving PII, as well as other breaches referenced in Paragraph 5.2.

b. Convenes and chairs the DoD Breach Response Team and, in coordination with the DoD Breach Response Team and the senior component officials for privacy (SCOPs), makes recommendations and final determinations on issues related to all major incidents involving PII (e.g., individual notification determinations and services provided to potentially affected individuals).

2.3. CHIEF, DEFENSE PRIVACY, CIVIL LIBERTIES, AND TRANSPARENCY DIVISION (DPCLTD).

Under the authority, direction, and control of the Director, DO&C, the Chief, DPCLTD:

a. Serves as the SCOP for the Office of the Director of Administration and Management.

b. Serves as a liaison between the affected DoD Component, the SAOP, and the DoD Breach Response Team.

c. Provides the SAOP with information regarding the numbers and types of breaches throughout DoD.

d. Provides the SAOP with an analysis of trends for all DoD breaches, along with possible preventive measures.

e. Provides guidance to the affected DoD Component SCOP and component privacy officer (CPO) as necessary and monitors the actions of the OSD or DoD Components in response to the breach.

f. Informs the SAOP upon learning there is a reasonable basis for determining that a major incident involving PII has occurred.

g. Develops and disseminates comprehensive breach reporting training materials and periodically assesses and updates the training materials in response to reported incidents.

2.4. DOD CHIEF INFORMATION OFFICER (CIO).

In addition to the responsibilities in Paragraph 2.8., the DoD CIO:

a. Ensures implementation of the responsibilities and procedures in this volume with respect to the security of DoD information systems.

b. Provides policy, standards, and guidance in accordance with DoD Directive 5144.02.

2.5. DOD SENIOR INFORMATION SECURITY OFFICER (SISO).

Under the authority, direction, and control of the DoD CIO, and in accordance with DoDI 5400.11, OMB Memorandum M-17-12, and annual OMB Federal Information Security and Privacy Management guidance (e.g., OMB Memorandum M-21-02 for Fiscal Year 2021), the DoD SISO:

a. Serves as the principal information technology and cybersecurity point of contact for major incidents involving PII.

b. Evaluates the effectiveness of information security measures in place to protect the PII and associated information systems that are the subject of a breach or potential breach.

c. Determines the likelihood or extent of incidents involving PII that may constitute major incidents, including the data sets potentially compromised and the number of individuals potentially affected.

d. Evaluates the effectiveness of information security mitigating actions following a major incident involving PII, or potential major incident involving PII.

e. Ensures that system security authorization documentation clearly defines the roles and responsibilities of contractors that operate DoD information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII on behalf of the DoD.

f. Ensures that breaches reported to DoD Component security operations centers (SOCs) or equivalents are, in turn, properly reported by the SOCs or equivalents to the United States Cyber Command (USCYBERCOM). Ensures information technology breaches are properly reported by USCYBERCOM to the Cybersecurity and Infrastructure Security Agency (United States

Computer Emergency Readiness Team (US-CERT)) and the OMB Office of the Federal CIO, as appropriate, in accordance with OMB Memorandums M-17-12 and annual OMB Federal Information Security and Privacy Management guidance.

g. Ensures that quarterly status reports on breaches reported to the SOCs during the fiscal year are provided to the SAOP in accordance with OMB Memorandum M-17-12.

2.6. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE.

In addition to the responsibilities in Paragraph 2.8., the General Counsel of the Department of Defense:

a. Provides legal advice to the DoD Breach Response Team.

b. Advises on whether the facts concerning a breach support a determination that a major incident involving PII has occurred.

c. Provides guidance on breach reporting obligations to the required congressional committees pursuant to Chapter 35, Subchapter II, of Title 44, U.S.C., also known and referred to in this volume as the "Federal Information Security Modernization Act of 2014 (FISMA)," and Section 1639 of Public Law 115-232 (codified at Section 2224 note of Title 10, U.S.C.), "Procedures and Reporting Requirement on Cybersecurity Breaches and Loss of Personally Identifiable Information and Controlled Unclassified Information."

d. Advises on the appropriateness of individual notification to those potentially affected by a breach.

e. Advises on the appropriateness of notification to the media and public concerning incidents involving PII.

2.7. ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS.

In addition to the responsibilities in Paragraph 2.8., the Assistant Secretary of Defense for Legislative Affairs:

a. Provides guidance when major incidents involving PII are reported to Congress and reviews and oversees the transmission of required reports to Congress.

b. Serves as the interface between DoD and Congress for congressional inquiries arising from incidents involving PII.

2.8. ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS.

In addition to the responsibilities in Paragraph 2.8., the Assistant to the Secretary of Defense for Public Affairs provides guidance on communicating to the media and public concerning major

incidents involving PII, as well as other breaches that may generate public or media interest, and communicates with the media and public concerning incidents involving PII when appropriate.

2.9. OSD AND DOD COMPONENT HEADS.

OSD and DoD Component heads:

a. Designate a SCOP in accordance with DoDI 5400.11 to ensure implementation of this volume in accordance with the roles and responsibilities outlined in Section 5.

b. Ensure the SCOP and any other component personnel tasked with preventing, responding to, or mitigating incidents involving the loss of PII are properly trained and resourced to execute their responsibilities.

c. Ensure all necessary privacy risks associated with any activities that involve the creation, collection, use, process, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems are evaluated. Ensure proper privacy and security controls are implemented, including clearly outlined incident reporting responsibilities in all information systems, information technology hosting agreements, and contracts in accordance with DoDI 5400.11.

2.10. COMMANDER, USCYBERCOM.

In addition to the responsibilities in Paragraph 2.8., the Commander, USCYBERCOM, reports suspected or confirmed information technology breaches to the Cybersecurity and Infrastructure Security Agency (i.e., US-CERT) and the OMB Office of the Federal CIO in accordance with the US-CERT Federal Incident Notification Guidelines (2017) and annual OMB Federal Information Security and Privacy Management guidance.

SECTION 3: SAOP ROLES AND RESPONSIBILITIES

The SAOP, as the DoD Breach Response Team Chair:

a. Convenes the team when appropriate, or at least once per fiscal year to hold a tabletop exercise.

(1) The purpose of the tabletop exercise is to test the Plan and to ensure that members of the team are familiar with the Plan and understand their specific roles.

(2) Testing breach response plans is an essential part of risk management and breach response preparation. The tabletop exercise should be used to practice a coordinated response to a breach, to further review and validate the Plan, and to identify potential weaknesses in response capabilities.

(3) If the SAOP and DoD Breach Response Team address an actual major incident involving PII during the fiscal year, with appropriate completion of after action reports and review of lessons learned, the tabletop requirement will be considered fulfilled.

b. Determines whether a major incident involving PII has occurred. To the maximum extent practicable, these determinations will be made in consultation with the affected SCOP and appropriate legal advisor(s).

c. Coordinates with financial management personnel to determine the resources that need to be allocated as a result of a major incident involving PII, and advise the DA&M accordingly.

d. Reports major incidents involving PII to the appropriate congressional committees and the Inspector General of the Department of Defense within 7 days from the date the breach is determined to be a major incident, in accordance with Section 3554 of Title 44, U.S.C., and related OMB guidance, including OMB Memorandums M-17-12 and annual OMB Federal Information Security and Privacy Management guidance. The report and any supplemental information should describe:

(1) Information known at the time of the report.

(2) Sensitivity of the details associated with the incident.

(3) Classification level of the information.

e. Ensures supplementary information about major incidents involving PII is provided to the appropriate congressional committees and the Inspector General of the Department of Defense no later than 30 days after the date the breach is determined to be a major incident. The supplement must address:

(1) A summary of information available about the breach, at the appropriate classification level, including how the breach occurred, based on information available on the date the SAOP submits the report.

(2) An estimate of the number of individuals affected by the breach, including an assessment of the risk of harm to affected individuals, based on information available to DoD officials on the date the SAOP submits the report.

(3) A description of any circumstances necessitating a delay in providing notice to affected individuals.

(4) An estimate of whether and when the agency will provide notice to affected individuals.

(5) The threats and threat actors, vulnerabilities, and impacts related to the incident.

(6) The risk assessments conducted of the affected information systems before the date on which the incident occurred.

(7) The status of compliance of the affected information system(s) with applicable security requirements at the time of the major incident.

(8) The detection, response, and remediation actions.

f. Reports breaches of PII affecting 250 or more DoD civilians or members of the Military Services to the appropriate congressional committees on a monthly basis in accordance with Paragraph 6.1.

g. Reviews the breach reports from the previous fiscal year, in coordination with the SCOPs as necessary, by the end of each calendar year. Considers whether the DoD should:

(1) Develop and implement new policies to protect DoD's PII holdings;

(2) Revise existing policies to protect DoD's PII holdings;

(3) Reinforce or improve training and awareness;

(4) Modify information sharing arrangements;

(5) Develop or revise documentation such as system of records notices (SORNs), privacy impact assessments, or privacy policies; or

(6) Use lessons learned to implement specific, preventative actions as necessary.

h. Reviews this volume annually, in coordination with the SCOPs, to confirm that it is current, accurate, reflects any changes in law, guidance, standards, DoD policy, procedures, staffing, or technology, and is updated as necessary. Documents the most recent review and submits an updated version to OMB when requested.

SECTION 4: DOD BREACH RESPONSE TEAM

4.1. MISSION.

a. The DoD Breach Response Team will meet when a major incident involving PII occurs in accordance with Section 3.

b. In the absence of an actual major incident, the DoD Breach Response Team will meet annually for a tabletop exercise, in accordance with Paragraph 3.a.

c. Analysis of incidents involving PII by the team will include the DoD CIO, SISO, mission or system owners, and the SCOP, as appropriate.

4.2. MEMBERSHIP.

a. SAOP, Chair.

b. SISO.

c. Chief, DPCLTD.

d. Senior representatives or designees of:

(1) USCYBERCOM.

(2) Office of the General Counsel of the Department of Defense.

(3) Office of the Assistant Secretary of Defense for Legislative Affairs.

(4) Office of the Assistant to the Secretary of Defense for Public Affairs.

e. Other personnel may be added to the team by the SAOP, as appropriate, including, but not limited to, senior intelligence officers, national security advisors, and law enforcement personnel.

SECTION 5: DOD COMPONENT BREACH RESPONSIBILITIES

5.1. DOD COMPONENT BREACH RESPONSIBILTIES.

a. General.

The SCOP is responsible for managing breaches at the DoD Component level with support from the CPO.

b. The SCOP.

The SCOP will:

(1) Review all information technology investment funding agreements involving PII, including data hosting agreements, to ensure all necessary privacy risk management efforts are accounted for in accordance with DoDI 5400.11.

(2) Ensure the Chief, DPCLTD, and the Commander, USCYBERCOM, are informed of all breaches within 48 hours of being notified that a breach has occurred to ensure a seamless flow of information throughout the DoD.

(3) Assess, in coordination with the appropriate DoD Component legal adviser, and in conjunction with the CPO, whether a major incident involving PII has occurred.

(4) Ensure a written assessment is completed concerning whether a major incident involving PII has occurred.

(a) The written assessment will be in accordance with OMB Memorandums M-17-12 and annual OMB Federal Information Security and Privacy Management guidance. It will be submitted to the Chief, DPCLTD, and the SAOP via e-mail, or within the Compliance and Reporting Tool (CART) at https://dpclo.osd.mil, or from a DPCLTD-designated breach reporting site.

(b) The SAOP may concur or non-concur with the assessment, or seek further information.

(c) In the event of a major incident or to resolve whether an incident should be considered a major incident, the SAOP will convene the DoD Breach Response Team to further assess the breach and make a recommendation or determination in accordance with Paragraphs 2.2 and 2.3.

(5) Conduct and document an assessment of the risk of harm to individuals potentially affected by a breach as outlined in Section 8.

(6) Determine how to best mitigate harm to individuals affected by a breach.

(7) Identify logistical capabilities needed to respond to a breach. Consult with the SAOP and DoD Component CIO, as needed, to determine any resource-intensive activities that may be necessary to provide notification, offer guidance, or provide services to individuals potentially affected by a breach.

(8) Consult with the DoD Component CIO to identify technical remediation and forensic analysis capabilities that exist within the DoD.

(9) Determine appropriate actions in response to a breach, to include countermeasures, additional staff resources when appropriate, and guidance or services to potentially affected individuals.

(10) Ensure that any required notification to law enforcement and the Office of Inspector General of the Department of Defense occurs in a timely manner as required by OMB Memorandum M-17-12.

(11) If it is determined that the breach was not a major incident involving PII, coordinate within the DoD Component concerned and determine appropriate actions to be taken. The SCOP will ensure breach information is provided to the DPCLTD as information becomes available, and will:

(a) Determine whether to notify individuals potentially affected by the breach. In considering whether to notify the affected individuals, the SCOP will consider:

1. The source of the breach.

2. Timeliness of the notification.

3. Content of the data.

4. Notification method.

5. Special considerations, including tailoring the notification for vulnerable populations, and how to notify individuals who are visually or hearing impaired.

(b) In the event of a breach by a DoD contractor, coordinate with appropriate DoD Component personnel to ensure the contractor complies with remediation measures required by the contract.

c. The CPO.

In addition to sharing information with the SCOP regarding the breach, the CPO, or designee, will ensure all required reporting occurs. The CPO, or designee, will:

(1) Report suspected or confirmed information technology breaches to the DoD Component SOC or equivalent. The SOC or equivalent will report such breaches through its chain of command to USCYBERCOM, which in turn reports to the OMB Office of the Federal CIO, as appropriate.

(2) Report the details on suspected and actual breaches to the SCOP within 24 hours of breach discovery. This includes a breach in any medium or form, including paper, oral, and electronic.

(3) Provide the SCOP with the SORNs, privacy impact assessments, and privacy notices applicable to the potentially compromised information.

(4) Document all breaches and actions taken in response to a breach using the Department of Defense (DD) Form 2959, "Breach of Personally Identifiable Information (PII) Report," and submit it to DPCLTD via CART at https://dpclo.osd.mil or a DPCLTD-designated breach reporting site within 48 hours of discovery of a breach.

(5) Promptly update initial reports in CART or a DPCLTD-designated breach reporting site as information becomes available and when pertinent decisions are made. This includes documenting whether affected individuals are being notified and, if so, the form of notification and number of affected individuals notified. Include lessons learned and corrective measures or preventative actions implemented. Provide a summary of any final administrative or disciplinary action taken against DoD personnel determined to be responsible for the breach.

(6) Close breach reports in CART or a DPCLTD-designated breach reporting site when all actions are complete, including documentation of lessons learned and any actions taken.

(7) Document any changes to DoD Component policies, training, or other documentation resulting from lessons learned. If there are specific challenges preventing the DoD Components from instituting remedies, document those challenges for auditing purposes.

5.2. DOD MULTI-COMPONENT OR MULTI-AGENCY BREACH RESPONSIBILTIES.

a. In the event a single breach affects multiple OSD or DoD Components, including a breach affecting a shared services arrangement among the Components, the SCOP of each affected Component will consult with the Chief, DPCLTD and the SAOP to determine which SCOP will assume the lead SCOP role as described in Paragraph 5.1., or if the Chief of DPCLTD or SAOP will assume the lead role. Lead role duties include coordination of the initial assessment of whether a breach constitutes a major incident and coordination of services provided to individuals potentially affected by a breach (e.g., credit monitoring).

b. In the event a single breach affects DoD and other Federal agencies, including a breach affecting shared services arrangements among federal agencies, the SCOP(s) will consult with the Chief, DPCLTD and the SAOP on whether the SCOP, Chief of DPCLTD, or SAOP will assume the role as central point of contact for the DoD.

c. In the event a single breach affecting multiple OSD or DoD Components or other Federal agencies is determined to be a major incident involving PII, the SAOP will assume the lead role as described in Paragraph 3.a.

SECTION 6: OTHER REPORTING REQUIREMENTS

6.1. SECTION 1639 BREACH REPORT.

a. General.

The DA&M will provide a monthly report on breaches of PII affecting 250 or more DoD civilians or Service members to the U.S. Senate and House Committees on Armed Services and the U.S. Senate and House Committees on Appropriations, Subcommittees on Defense, in accordance with Section 1639 of Public Law 115-232 (codified at Section 2224 note of Title 10, U.S.C.).

b. Report.

The monthly report will contain details of all breaches of PII affecting 250 or more DoD civilians or Service members submitted to the DPCLTD in the previous month. If no such breaches are reported to the DPCLTD in a given month, no report will be submitted to Congress for that month.

(1) Such reportable breaches on the Non-classified Internet Protocol Router Network (NIPRNET) will be communicated using DD Form 2959 and CART or a DPCLTD-designated breach reporting site. There is no additional reporting requirement for the DoD Component; however, DPCLTD may request follow-up information. The DPCLTD will prepare the monthly Section 1639 Breach Report for the DA&M to submit to Congress.

(2) Reportable breaches occurring on the SIPRNET will be communicated to the DPCLTD via e-mail at OSD.MC-ALEX.OCMO.MBX.PII-Breach@mail.smil.mil using the DD Form 2959. The DPCLTD will prepare a classified annex of the Section 1639 Breach Report for the DA&M to submit to Congress.

(3) Reportable breaches occurring on the JWICS will be communicated to the DPCLTD via e-mail at PII.Breach@osdj.ic.gov using the DD Form 2959. The DPCLTD will prepare a classified annex of the Section 1639 Breach Report for the DA&M to submit to Congress.

(4) The SAOP will coordinate the monthly report with appropriate offices, including the Deputy Comptroller, Budget and Appropriations Affairs, and the General Counsel of the Department of Defense.

(5) The Assistant Secretary of Defense for Legislative Affairs will submit the report to the appropriate congressional committees.

6.2. ANNUAL FISMA REPORTS.

a. General.

FISMA requires DoD to submit an annual report on the adequacy and effectiveness of information security policies, procedures, and practices, including major incidents involving PII.

b. Report.

The SAOP will include descriptions of DoD's implementation of the requirements in this volume in the annual FISMA report. At a minimum, the SAOP will:

(1) Confirm the DoD satisfied the requirements of this volume for training and awareness with respect to breach reporting or, if not, explain why the DoD did not satisfy the requirements and what steps the DoD will take to meet its requirements in the next reporting period.

(2) Submit the number of breaches reported within DoD during the reporting period, the number of breaches reported to the US-CERT, the number of breaches (as defined by OMB Memorandum M-17-12) that the DoD reported to Congress, as well as the number of potentially affected individuals.

(3) Review the Plan and certify that it has been reviewed and updated over the past 12 months, as appropriate.

(4) Identify the members of the DoD's Breach Response Team and identify those individuals who were removed from the team or added to the team over the past 12 months.

(5) Confirm that the DoD Breach Response Team participated in at least one tabletop exercise during the reporting period if it did not address an actual major incident with appropriate completion of after action reports and review of lessons learned, in accordance with Paragraph 3.a. If a tabletop exercise was not completed, explain why and what steps the DoD will take to ensure that a tabletop exercise is completed during the next reporting period.

SECTION 7: PREPARING FOR A BREACH

7.1. PRIVACY ACT ROUTINE USES REQUIRED FOR BREACH RESPONSE.

a. To facilitate DoD's response to a breach of its own records, all OSD and DoD Components will include a routine use into each SORN, as shown in Figure 1.

Figure 1. Routine Use for Breach of DoD Records

> To appropriate agencies, entities, and persons when (1) DoD suspects or has confirmed that there has been a breach of the system of records; (2) DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

b. To ensure that DoD is able to disclose records in its system of records that may reasonably be needed by another agency in responding to a breach, all OSD and DoD Components will incorporate a routine use into each SORN, as shown in Figure 2.

Figure 2. Routine Use for Assisting Another Federal Agency with Breach Responses

> To another federal agency or federal entity, when DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach; or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

7.2. CONTRACTS AND CONTRACTOR REQUIREMENTS FOR BREACH RESPONSE.

a. General.

DoD contracting personnel will ensure that contractual terms necessary for DoD to respond to a breach are uniform and consistently included in contracts when a contractor creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of PII on behalf of the DoD in accordance with Section 3554(a)(1)(A) of Title 44, U.S.C. To the extent that a cooperative agreement or other such instrument requires another organization or entity to perform such functions on behalf of the DoD, in accordance with Section 6305 of Title 31, U.S.C., the DoD will similarly ensure that such cooperative agreements and instruments include the terms in Paragraph 7.2.b.

b. Terms.

At a minimum, contracts will include terms that:

(1) Require the contractor to cooperate with and exchange information with DoD officials to effectively report and manage a suspected or confirmed breach.

(2) Require contractors and subcontractors (at any tier) to properly safeguard and encrypt PII in accordance with OMB Circular No. A-130 and other applicable policies and to comply with all DoD-specific policies for protecting PII.

(3) Require regular training for contractors and subcontractors (at any tier) on how to identify and report a breach.

(4) Require contractors and subcontractors (at any tier) to report a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay.

(5) Require contractors and subcontractors (at any tier) to maintain capabilities to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector.

(6) Allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with OMB Memorandum M-17-12 and this volume, and to assist with responding to a breach.

(7) Identify roles and responsibilities, in accordance with OMB Memorandum M-17-12 and this volume.

(8) Explain that a report of a breach, by itself, will not be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII.

(9) Require the contractor to notify individuals potentially affected by a breach as explained in this volume, subject to the DoD's guidance, review, direction, and approval, and in accordance with contract language.

(10) Ensure that any required countermeasures are consistent with OMB Memorandum M-16-14 which, except under limited circumstances, requires the use of General Services Administration's (GSA) identity protection services blanket purchase agreements (BPAs).

(a) GSA has awarded government-wide Federal Supply Schedule BPAs for identity monitoring, credit monitoring, and other related services.

(b) These BPAs give access to a vetted pool of well-qualified contractors capable of providing the comprehensive services needed to mitigate the risk of harm to individuals potentially affected by a breach, as well as other personnel security matters.

c. Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) Clauses.

At a minimum, contracts will include, and the contracting officer will insert in solicitations and contracts, the following clauses when the design, development, or operation of a system of records on individuals is required to accomplish a DoD function:

(1) DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (December 2019), https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.

(2) DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls (October 2016), https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm.

(3) FAR 52.224-1 Privacy Act Notification (April 1984) as prescribed in 24.104, https://www.acquisition.gov/content/52224-1-privacy-act-notification.

(4) FAR 52-224-2 Privacy Act (April 1984), https://www.acquisition.gov/content/52224-2-privacy-act.

(5) FAR 52.224-3 Privacy Training (January 2017), https://www.acquisition.gov/far/52.224-31.

(6) FAR 52.239-1 Privacy or Security Safeguards (August 1996), https://www.acquisition.gov/far/52.239-1.

(7) FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems, (June 2016), https://www.acquisition.gov/far/52.204-21-0.

7.3. GRANT AND GRANT RECIPIENT REQUIREMENTS FOR BREACH RESPONSE.

When a grant recipient uses or operates a DoD information system or creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of PII within the scope of a DoD award, the DoD grantor will:

a. Ensure the grant recipient has procedures in place to respond to a breach of the DoD information system or DoD-related PII and include terms and conditions requiring the recipient to notify promptly the DoD awarding officials in the event of a breach.

b. Ensure the procedures are consistent with Section 7.2, as applicable, and promote cooperation and the free exchange of information with DoD awarding officials, as needed, to properly escalate, refer, and respond to a breach.

SECTION 8: ASSESSING AND MITIGATING THE RISK OF HARM AND NOTIFYING AFFECTED INDIVIDUALS

8.1. RISK OF HARM TO INDIVIDUALS POTENTIALLY AFFECTED BY A BREACH.

a. General.

In order to properly escalate and tailor breach response activities, the affected DoD Component's SCOP, as required by Paragraph 5.1.b., in coordination with the CPO, will conduct and document a risk assessment of the harm to individuals potentially affected by a breach, including the factors the DoD Component will consider when assessing the risk. When the breach involves a major incident or multiple components, the SCOP and CPO will engage in consultation with the SAOP and the Breach Response Team, as appropriate.

b. Risk of Harm to Individuals.

When assessing the risk of harm to individuals potentially affected by a breach, consider the potential harms that could result from the loss or compromise of PII. Such harms may include:

(1) Breach of confidentiality or fiduciary responsibility;

(2) Potential for blackmail;

(3) Disclosure of private facts;

(4) Mental pain and emotional distress;

(5) Financial harm;

(6) Disclosure of contact information for victims of abuse;

(7) Potential for secondary uses of the information that could result in fear or uncertainty; or

(8) Unwarranted exposure leading to humiliation or loss of self-esteem.

c. Risk of Harm to the Government.

Consider any and all risks relevant to the breach, which may include risks to the DoD, DoD information systems, DoD programs and operations, the Federal Government, or national security.

8.2. FACTORS FOR ASSESSING THE RISK OF HARM TO POTENTIALLY AFFECTED INDIVIDUALS.

a. General.

At a minimum, consider the following factors when assessing the risk of harm to individuals potentially affected by a breach:

(1) Nature and Sensitivity of the PII Potentially Compromised by the Breach.

Include the actual and potential harms that an individual experiences or may experience from the compromise of the particular type of PII.

(2) Likelihood of Access to and Use of PII.

Include whether the PII was properly encrypted or rendered partially or completely inaccessible by other means.

(3) Type of Breach.

Include the circumstances of the breach, as well as the actors involved and their intent.

b. Nature and Sensitivity of PII.

At a minimum, consider the following factors when assessing the nature and sensitivity of PII potentially compromised by a breach:

(1) Data Elements.

Analyze the sensitivity of each individual data element, as well as the sensitivity of all the data elements together.

(a) Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual because of their greater potential for misuse and harm to the individual. These data elements include, but are not limited to:

1. Social Security numbers (SSNs).
2. Passport numbers.
3. Driver's license numbers.
4. State identification numbers.
5. Bank account numbers.
6. Biometric identifiers.
7. Passwords.

(b) In addition to evaluating the sensitivity of each data element, be aware that the compromise of multiple data elements together may present an increased risk of harm to the individual when combined. For example, date of birth, place of birth, address, and gender may not be particularly sensitive alone, but when combined would pose a greater risk of harm to the individual.

(c) Also consider data that has been potentially compromised in previous breaches, as well as any other available information, public or agency-specific, that may increase the risk of harm to the individuals involved.

(2) Context.

(a) When assessing the nature and sensitivity of PII potentially compromised by a breach, consider the context. The context includes the purpose for which the PII was collected, maintained, and used.

(b) This assessment is critical because the same information in different contexts can reveal additional information about the impacted individuals. For example, a list of personnel and their associated office phone numbers may not be particularly sensitive. However, the same list of personnel and their associated office phone numbers on a list of personnel who hold sensitive positions within a DoD law enforcement agency or a group of routinely deployed DoD personnel is sensitive information. Similarly, the same list of names and associated phone numbers on a list of individuals along with information about a medical condition is also sensitive.

(3) Private Information.

Include the extent to which the PII, in a given context, may reveal particularly private information about an individual. Evaluate the extent to which the PII constitutes information an individual would generally keep private. Such private information may not present a risk of identity theft or other criminal conduct, but may pose a risk of harm such as embarrassment, blackmail, or emotional distress. Examples of private information include:

(a) Derogatory personnel or criminal information.

(b) Personal debt and finances.

(c) Medical conditions.

(d) Treatment for mental health.

(e) Pregnancy related information, including pregnancy termination.

(f) Sexual history or sexual orientation.

(g) Adoption or surrogacy information.

(h) Passwords.

(i) Immigration status.

(4) Vulnerable Populations.

Include the extent to which the PII identifies or disproportionately impacts a particularly vulnerable population. Consider whether the potentially affected individuals are from a particularly vulnerable population that may be at greater risk of harm than the general population. Potentially vulnerable populations include, but are not limited to:

(a) Children.

(b) Active duty military.

(c) Government officials in sensitive positions.

(d) Senior citizens.

(e) Individuals with disabilities.

(f) Confidential informants.

(g) Witnesses.

(h) Certain populations of immigrants.

(i) Non-English speakers.

(j) Victims of certain crimes such as sexual assault, identity theft, child abuse, trafficking, domestic violence, or stalking.

(5) Permanence.

Include the continued relevance and utility of the PII over time and whether it is easily replaced or substituted. Consider the permanence of the PII. This includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy or utility as it ages.

(a) For example, an individual's health insurance identification number can be replaced. However, information about an individual's health, such as family health history or chronic illness, may remain relevant for an individual's entire life, as well as for the lives of his or her family.

(b) Special consideration is warranted when a breach involves biometric information including fingerprints, hand geometry, retina or iris scans, and DNA or other genetic information. When considering the nature and sensitivity of biometric information, factor in the known current uses of the information and consider that, with future advancements in science and technology, biometric information could have many additional uses not yet contemplated.

c. Likelihood of Access to and Use of PII.

Consider the following when assessing the likelihood of access to and use of PII potentially compromised by a breach.

(1) Security Safeguards.

Include whether the PII was properly encrypted or rendered partially or completely inaccessible by other means. When assessing the likelihood of access to and use of PII potentially compromised by a breach, the DoD Component CIO will evaluate the implementation and effectiveness of security safeguards protecting the information. Security safeguards may significantly reduce the risk of harm to potentially affected individuals, even when the PII is particularly sensitive. The DoD Component CIO will consider each of the employed security safeguards on a case-by-case basis and take into account whether the type, value, or sensitivity of the information might motivate a malicious actor to put time and resources towards overcoming those safeguards.

(a) When evaluating the likelihood of access and use of encrypted PII potentially compromised by a breach, the DoD Component CIO, in coordination with the DoD CIO, SCOP, SAOP, and SISO, as necessary, will consider:

1. Whether encryption was in effect.

2. The degree of encryption.

3. At what level the encryption was applied.

4. Whether decryption keys were controlled, managed, and used.

(b) There are many ways to encrypt information, and different technologies provide varying degrees of protection. Consider whether encryption was applied:

1. At the device-level.

2. At the file-level.

3. To information at rest and/or in transmission.

(c) The protection provided by encryption may be undermined if keys, credentials, or authenticators used to access encrypted information are compromised.

(d) The SCOP will consult with the SAOP, SISO, and other technical experts, as appropriate, to ascertain whether information was properly encrypted in accordance with OMB Circular A-130 requirements.

(e) The PII potentially compromised by a breach also may be rendered partially or completely inaccessible by implementation of other security safeguards such as:

1. Redaction.

2. Data masking.

3. Remote wiping of a connected device.

4. Physical security safeguards such as a locked case securing documents or devices.

(2) Format and Media.

The SCOP, in coordination with the DoD Component CIO, will evaluate whether the format or media of the PII may make its use difficult, resource-intensive, and time consuming.

(a) The format of the PII or the media on which it is maintained may make the PII more susceptible to a crime of opportunity. For example, a spreadsheet on a portable USB flash drive does not require special skills or knowledge to access and an unauthorized user could quickly search for specific data fields. Conversely, magnetic tape cartridge used for backing up servers that is 1 of a set of 30 and contains large amount of unstructured PII would require special expertise and equipment to access and use the information.

(b) The SCOP will also consider the type, value, or sensitivity of the PII. If the PII is particularly valuable, it may increase the likelihood of access and use regardless of its format or media. The value of information may outweigh the difficulty and resources needed to access the information for misuse.

(3) Duration of Exposure.

When assessing the likelihood of access and use of PII potentially compromised by a breach, consider the amount of time that the PII was exposed. PII that was exposed for an extended period of time is more likely to have been accessed or used by unauthorized persons.

(4) Evidence of Misuse.

When assessing the likelihood of access and use of PII potentially compromised by a breach, determine whether there is evidence of misuse. In some situations, it may be determined with a high degree of certainty that PII has been or is being misused. Evidence may indicate that identity theft has already occurred as a result of a specific breach or that PII is appearing in unauthorized external contexts. For example, law enforcement may confirm that PII is appearing on a website dedicated to the sale of stolen PII and may determine that there is strong evidence of misuse. Conversely, a forensic analysis of a recovered device may reveal that PII was not accessed.

d. Type of Breach.

Consider the following when determining the type of breach:

(1) Intent.

When assessing the risk of harm to individuals potentially affected by a breach, consider whether the breach was intentional, unintentional, or whether the intent is unknown.

(a) If the breach was intentional, determine whether the information was the target, or whether the target was the device itself, like a mobile phone or laptop, and whether the compromise of the information was incidental. Examples of an intentional breach include theft of a device storing PII from a car or office, the unauthorized intrusion into a government network that maintains PII, or an employee looking up a celebrity's file in a DoD database out of curiosity. While the risk of harm to individuals may often be lower when the information was not the target, the potential for a significant risk of harm to individuals may still exist.

(b) The risk of harm to individuals may be lower when a breach is unintentional, either by user error or sometimes by failure to follow DoD policy. However, that is not always the case, and the SCOP must conduct a case-by-case assessment to determine the risk of harm. Examples of an unintentional breach include an employee accidentally e-mailing another individual's PII to the wrong e-mail address or storing personnel files in a shared folder that was believed to be access-controlled but actually was not.

(c) In many circumstances, it may not be clear whether a breach was intentional or unintentional. For example, if an employee realizes their mobile device is missing, it may be that it was stolen intentionally or lost accidentally. Similarly, a shipment of files containing PII that never arrives at its destination may have been unintentionally lost or may have been targeted by a malicious actor and intercepted.

(2) Recipient.

When assessing the risk of harm to individuals potentially affected by a breach, consider whether the PII was disclosed to a known or unknown recipient, and the trustworthiness of a known recipient. In some cases, the DoD may know who received the compromised PII. This information, when available, may help the SCOP assess the likely risk of harm to individuals. For example, a breach is often reported by a recipient who receives information they should not have. This may be an indication of a low risk of harm to individuals, particularly when the recipient is another DoD employee.

(a) One common type of low-risk breach is when an employee sends an individual's PII via e-mail to another employee in the same DoD Component who does not have a need to know that PII for their duties. In many such cases it may be reasonable to conclude that there is negligible risk of harm. Even where PII is inadvertently sent to an individual outside the DoD, the risk of harm may be minimal if it is confirmed that the individual is known to the DoD, acknowledged receipt of the PII, did not forward or otherwise use the PII, and the PII was properly, completely, and permanently deleted by the recipient. This is a breach that must be reported and appropriately responded to, but the risk of harm is low enough that the response often does not necessitate that the DoD Component notify or provide services to the individual whose PII was compromised.

(b) Conversely, if analysis reveals that the PII is under control of a group or person who is either untrustworthy or known to exploit compromised information, the risk of harm to the individual is considerably higher.

(c) In many cases there will be no information indicating that the compromised or lost PII was ever received or acquired by anyone. In such circumstances, the SCOP will rely upon other factors in this volume.

8.3. MITIGATING THE RISK OF HARM TO INDIVIDUALS POTENTIALLY AFFECTED BY A BREACH.

a. General.

Once the SCOP assesses the risk of harm to individuals potentially affected by a breach, he or she will consider, in coordination with the CPO, how best to mitigate the identified risks. The SCOP will advise the DoD Component's senior leadership on whether to take countermeasures, offer guidance, or provide services to individuals potentially affected by a breach. When the breach involves a major incident or involves multiple components, the SCOP and CPO will engage in appropriate consultation with the SAOP and the Breach Response Team, as appropriate.

b. Countermeasures, Guidance, and Services.

Because each breach is fact-specific, the decision of whether to take countermeasures, offer guidance, or provide services to potentially affected individuals will depend on the circumstances of the breach. Consider the assessed risk of harm conducted in accordance with Paragraphs 8.1 and 8.2.

(1) The SCOP will decide, in coordination with the CPO, whether to take countermeasures, offer guidance, or provide services to individuals potentially affected by a breach.

(2) The SCOP will determine and document the actions that the DoD Component will take to mitigate the risk of harm to individuals potentially affected by a breach. These actions can include:

(a) Countermeasures.

Countermeasures may not always prevent harm to potentially affected individuals, but may limit or reduce the risk of harm. For example, if credit card information is potentially compromised, the DoD Component may proactively notify appropriate banks so they can monitor the associated accounts or reissue of the lines of credit using new accounts. Other countermeasures may also include expiring potentially compromised passwords or placing an alert in a database containing potentially compromised PII.

(b) Guidance.

The type of guidance provided to mitigate the risk of harm to individuals will necessarily depend on the potentially compromised information. Use the information available at https://www.identitytheft.gov/Info-Lost-or-Stolen as a baseline when drafting guidance.

1. There are several steps individuals can take to mitigate their own risk of harm resulting from a breach. These include:

a. Setting up fraud alerts or credit freezes.

b. Changing or closing accounts.

c. Taking advantage of services made available by the Federal Trade Commission.

2. The Federal Trade Commission provides specific guidance for when a breach involves SSNs, payment credit information, bank accounts, driver's licenses, children's information, and account credentials.

3. The DoD Component may advise individuals to change passwords and encourage the use of multi-factor authentication for account access. When choosing guidance to mitigate the risk of harm, the SCOP should consider the guidance options included in Appendix II of OMB Memorandum M-17-12.

(c) Services.

The SCOP will determine, in coordination with the CPO, if there are services that are appropriate to provide to potentially affected individuals. Many of the services currently available in today's marketplace only mitigate risks of financial identity theft, and even the most comprehensive services are unable to eliminate the potential harms resulting from the evolving threat and risk landscape. The SCOP will identify those services that best mitigate the specific risk of harm resulting from the particular breach when selecting services.

1. If the SCOP determines, in coordination with the CPO, that no service currently available appropriately mitigates a specific risk of harm, he or she may choose not to provide services to potentially affected individuals. Choosing not to provide services is a decision separate from the decision to provide notification and there may be circumstances where potentially affected individuals are notified but not provided services.

2. When choosing identity monitoring, credit monitoring, and other related services to mitigate the risk of harm to individuals potentially affected by a breach, the SCOP will take advantage of GSA BPAs in accordance with OMB Memorandum M-16-14. For details on the Identity Protection Services BPA (Identity Protection Services Special Item Number on the Multiple Awards Schedule), including task order instructions, offered services, authorized users, order dollar value limitation, the inclusion of DoD-specific terms, and ordering periods, visit https://www.gsa.gov/ipsbpa.

8.4. NOTIFYING INDIVIDUALS POTENTIALLY AFFECTED BY A BREACH.

a. General.

The SCOP is responsible, in coordination with the CPO, for advising its senior leadership on whether and when to notify individuals potentially affected by a breach. The decision of whether to notify individuals depends on the specific circumstances of the breach and the assessed risk of harm conducted.

(1) For breaches not determined to be major incidents, the SCOP is responsible, in conjunction with the CPO, for making a decision regarding whether to provide notification.

(2) When a breach constitutes a major incident, the SCOP will ensure that appropriate consultation with the SAOP and the DoD Breach Response Team occurs in accordance with this volume. The SCOP may consider delay in notifying individuals potentially affected by a breach if the notification would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions in accordance with OMB Memorandum M-17-12. Any recommendation to delay notification will be sent to the SAOP.

b. Decision Criteria and Factors.

The decision to offer guidance, initiate countermeasures, or provide services to individuals potentially affected by a breach will require the DoD Components to notify those individuals of both the breach and the steps taken to mitigate any identified risks. For example, if the decision was made to provide identity and credit monitoring to individuals potentially affected by a particular breach, the DoD Component will need to notify those individuals so they can use the service being provided.

(1) DoD Components may choose to notify individuals even when not providing a specific service. For example, a DoD Component may notify individuals that their passwords are potentially compromised by a breach and offer guidance but not services.

(2) DoD Components should balance the need for transparency with concerns about over-notifying individuals. Notification may not always be helpful to the potentially affected individuals, and DoD Components should exercise care to evaluate the benefit of providing notice to individuals or notifying the public.

(3) DoD Components must coordinate with the Defense Health Agency Privacy and Civil Liberties Office for all matters related to protected health information covered by DoDI 6025.18 and DoDM 6025.18, in accordance with DoDI 8580.02. In circumstances where multiple notification requirements apply to a breach, DoD Components should provide a single notice to potentially affected individuals that complies with the guidance in this volume as well as any other notification requirements.

(4) When the determination has been made that it is necessary to notify individuals potentially affected by a breach, the SCOP, in coordination with the CPO, will need to determine:

(a) Source of the Notification.

1. When notification is necessary, helpful, or otherwise required, the SCOP, or other more senior-level individual within the DoD Component, should notify potentially affected individuals. When a breach involves a well-known DoD Component or well-known system, the Component head should issue the notification.

2. When PII created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed by a contractor, or by a subcontractor, on behalf of the DoD is involved in a breach, DoD may require the contractor to notify any potentially affected individuals in accordance with Paragraph 7.2 of this volume and Paragraph 2.8.e. of DoDI 5400.11.

(b) Timeliness of the Notification.

1. Notify individuals potentially affected by a breach as expeditiously as practicable and without unreasonable delay. Balance the timeliness of the notification with the need to gather and confirm information about a breach and assess the risk of harm to potentially affected individuals.

2. Notification to individuals potentially affected by a breach may be delayed after proper consultation with the SAOP and appropriate DoD coordination with the Department of Justice, an appropriate Intelligence Community element, or the Department of Homeland Security, if the notification would:

a. Disrupt a law enforcement investigation;

b. Endanger national security; or

c. Hamper security remediation actions.

(c) Contents of the Notification.

1. Notification to individuals potentially affected by a breach should be concise and be written in plain language. Avoid using generic or repetitive language and tailor the notification to the specific breach. Include whether to draft different notifications for different populations potentially affected by a breach.

2. At a minimum, notifications will, to the extent possible, include:

a. A brief description of what happened, including the date(s) of the breach and of its discovery.

b. A description of the types of PII compromised by the breach (e.g., full name, SSN, date of birth, home address, account number, and disability code).

c. A statement of whether the information was encrypted or protected by other means, when it is determined that disclosing such information would be beneficial to

potentially affected individuals and would not compromise the security of the information system.

d. Guidance to potentially affected individuals on how they can mitigate their own risk of harm, countermeasures the DoD Component is taking, and services the DoD Component is providing, if any.

e. Steps the DoD or DoD Component is taking, if any, to investigate the breach, to mitigate losses, and to protect against a further breach.

f. Whom potentially affected individuals should contact at DoD for more information, including a telephone number (preferably toll-free), e-mail address, and postal address.

3. DoD Components may want to provide additional details in a frequently asked questions format on their website or via an enclosure. The frequently asked questions on the DoD Component's website may be beneficial because they can be easily updated, contain links to more information, provide more tailored information than the formal notification, and can be easily translated into multiple languages. For a breach that potentially affects a large number of individuals, as appropriate, DoD Components should establish toll-free call centers staffed by trained personnel to handle inquiries.

(d) Method of the Notification.

The best method for providing notification will potentially depend on the number of individuals affected, the available contact information, and the urgency with which the individuals need to receive the notification.

1. First-Class Mail.

a. First-class mail notification to the last known mailing address of the individual should be the primary means of notification. If DoD Components have reason to believe the address is no longer current, DoD Components should take reasonable steps to update the address by consulting with the Defense Manpower Data Center, Defense Civilian Personnel Data System, and other government agencies such as the U.S. Postal Service, as appropriate.

b. Notifications generally should be sent separately from any other mailing so it is obvious to the recipient. If the DoD Component that experienced the breach uses another agency or entity to facilitate mailing, care should be taken to ensure that the DoD Component that suffered the loss is clearly identified as the source of the notice, and not the agency or entity who is facilitating the mailings.

c. Label the front of the envelope to alert the recipient to the importance of its contents and to reduce the resemblance to advertising mail; the envelope should be marked with the DoD Component's name. Anticipate mail returned as undeliverable and have procedures in place for how to provide secondary notification.

2. Telephone.

a. Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification or when a small number of individuals are affected.

b. Telephone notification should be simultaneous with written notification by first-class mail.

3. E-mail.

a. While e-mail is not recommended as the primary form of notification, in limited circumstances it may be appropriate. E-mail notification, especially to or from a non-government e-mail address, is not recommended due to the high risk of malicious e-mail attacks that are often launched when attackers hear about PII breaches. E-mails may be automatically routed to spam or junk folders and may not reach the intended recipients. Individuals are often uncertain of the legitimacy of the e-mail and may not open the notification.

b. If the individuals affected by a PII breach are internal to the DoD, it may be appropriate for DoD Components to use an official e-mail address to notify a small number of employees, contractors, or interns via their official DoD e-mail addresses.

(e) Substitute Notification.

Substitute notifications may be provided if the DoD Component does not have sufficient contact information to provide notification, and also as supplemental notification for any breach to keep potentially affected individuals informed. This type of notice may also be beneficial if the DoD Component needs to provide an immediate or preliminary notification in the wake of a high-profile breach when notification is particularly time-sensitive.

1. A substitute notification should consist of a visible posting of the notification on the home page of the DoD Component's website or notification to major print and broadcast media, including media in areas where the potentially affected individuals reside. Notification to media should include a toll-free phone number or an e-mail address that an individual can use to learn whether their personal information is affected by the breach.

2. In instances where there is an ongoing investigation and the facts and circumstances of a breach are evolving, DoD Components should consider whether it is appropriate to establish an ongoing communication method for interested individuals to automatically receive updates.

3. Depending on the individuals potentially affected and the specific circumstances of a breach, it may be necessary to provide notifications in more than one language.

(f) Special Considerations.

When a breach potentially affects a vulnerable population, it may become necessary to provide a different type of notification to that population, or provide a notification when it would not otherwise be necessary.

1. There may be instances when notices are provided to individuals other than those whose PII was potentially compromised (e.g., when the individual whose information was potentially compromised is a child). Notification to the child's legal guardian(s) may be provided. Special care may be required to determine the appropriate recipient in these cases.

2. DoD Components should give special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 794d of Title 29, U.S.C., also known as "Section 508 of the Rehabilitation Act of 1973" or "Section 508." Accommodations may include establishing a telecommunications device for the deaf or ensuring postings on the DoD Component's website are Section 508 compliant.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
BPA	blanket purchase agreement
CART	Compliance and Reporting Tool
CIO	Chief Information Officer
CPO	component privacy officer
DA&M	Director of Administration and Management
DD	Department of Defense (when referring to form only)
DFARS	Defense Federal Acquisition Regulation Supplement
DNA	deoxyribonucleic acid
DO&C	Directorate for Oversight and Compliance
DoDI	DoD instruction
DPCLTD	Defense Privacy, Civil Liberties, and Transparency Division
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Modernization Act
GSA	General Services Administration
JWICS	Joint Worldwide Intelligence Communication System
NIPRNET	Non-classified Information Protocol Network
OMB	Office of Management and Budget
PII	personally identifiable information
SAOP	senior agency official for privacy
SCOP	senior component official for privacy
SIPRNET	SECRET Internet Protocol Router Network
SISO	senior information security officer
SOC	security operations center
SORN	system of records notice
SSN	Social Security number
USB	universal serial bus
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USCYBERCOM	United States Cyber Command

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this volume.

TERM	DEFINITION
breach	Defined in OMB Memorandum M-17-12.
countermeasure	The employment of devices or techniques by the DoD that may limit or reduce the risk of harm to individuals potentially affected by a breach**.**
CPO	A federal employee who is responsible for the day-to-day management of the DoD Component privacy program.
incident	Defined in OMB Memorandum M-17-12.
individual	Defined in the Privacy Act of 1974.
maintain	Defined in the Privacy Act of 1974.
major incident	A breach that 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 the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. While DoD or the DoD Component will assess each breach on a case-by-case basis to determine whether the breach meets the definition of a major incident, a determination of major incident is required for any unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to the PII of 100,000 or more individuals. Defined in annual OMB Federal Information Security and Privacy Management guidance (e.g., OMB Memorandum M-21-02 for Fiscal Year 2021).
PII	Defined in OMB Circular No. A-130.
routine use	Defined in the Privacy Act of 1974.
SCOP	A member of the senior executive service or general officer/flag officer acting on behalf of the SAOP and responsible for the overall implementation of the privacy and civil liberties programs in his or her DoD or OSD Component.
SORN	Defined in OMB Circular No. A-108.

REFERENCES

Cybersecurity and Infrastructure Security Agency, "US-CERT Federal Incident Notification Guidelines (2017)," April 1, 2017

Defense Federal Acquisition Regulation Supplement, current edition

Deputy Secretary of Defense Memorandum, "Re-establishment of the Assistant to the Secretary of Defense for Intelligence Oversight and the Director of Administration and Management," January 11, 2021

DoD Directive 5105.53, "Director of Administration and Management (DA&M)," February 26, 2008

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019

DoD Instruction 6025.18, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs," March 13, 2019

DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015

DoD Manual 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DOD Health Care Programs," March 13, 2019

Federal Acquisition Regulation, current edition

Office of Management and Budget Circular No. A-130, "Managing Information as a Strategic Resource," July 28, 2016

Office of Management and Budget Memorandum M-16-14, "Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response," July 1, 2016

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

Office of Management and Budget Memorandum M-21-02, "Fiscal Year 2020-2021-Guidance on Federal Information Security and Privacy Management Requirements," November 9, 2020

Public Law 115-232, Section 1639 (codified at Section 2224 note of Title 10, U.S.C.), "Procedures and Reporting Requirement on Cybersecurity Breaches and Loss of Personally Identifiable Information and Controlled Unclassified Information," August 13, 2018

United States Code, Title 5, Section 552a (also known as the "Privacy Act of 1974," as amended)

United States Code, Title 29, Section 794d (also known as "Section 508 of the Rehabilitation Act of 1973")

United States Code, Title 31, Section 6305

United States Code, Title 44