OFFICE OF THE DEPUTY CHIEF MANAGEMENT OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, DC 20301-9010

OVERSIGHT AND
COMPLIANCE

August 28, 2017

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARIES OF DEFENSE
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Designation of Senior Component Officials for Privacy and Establishment of Roles and Responsibilities

The Department of Defense (DoD) has a long-standing commitment to protect the privacy and civil liberties of individuals and safeguard the personal information that it maintains as it carries out its missions and agency operations. This memorandum's purpose is to provide information on updates to federal agency privacy policies and requirements and request a designation or re-designation of a Senior Component Official for Privacy (SCOP) consistent with the requirements in DoD Directive 5400.11, "DoD Privacy Program."

Executive Order (E.O.) 13719, dated February 9, 2016, established a Federal Privacy Council (FPC), creating an interagency forum to improve the privacy practices of the federal government. One of the goals of the FPC is to encourage agencies to develop and implement strategic and comprehensive privacy programs to more effectively address today's complex privacy issues. E.O. 13719 requires the head of each federal agency to designate a Senior Agency Official for Privacy (SAOP) with the experience and skills necessary to manage an agency-wide privacy program and to serve as a member of the FPC. Consistent with this requirement, the Secretary of Defense, through the Deputy Chief Management Officer (DCMO), has designated me to serve as the DoD SAOP.

Additionally, the Office of Management and Budget (OMB) recently updated two important federal agency guidance documents: OMB Circular A-130, "Managing Information as a Strategic Resource," dated July 28, 2016, and OMB Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," dated

December 23, 2016. OMB Circular A-130 updates and substantially expands the role and responsibilities of the SAOP as well as other agency officials in managing information. This circular includes procedures for information security and emphasizes the risk management framework as a key process that requires collaboration between the SAOP and the Chief Information Officer (CIO)/Chief Information Security Officer, which will help to ensure protection of personally identifiable information (PII) throughout the life cycle of information systems. OMB Circular A-108 revises agency responsibilities for implementing the review, reporting, and publication requirements of the Privacy Act of 1974 and related OMB policies.

To ensure the effective oversight and implementation of the DoD privacy program, I request that you designate or re-designate a SCOP by September 21, 2017, and that your designation be sent to the Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD) at osd.ncr.odcmo.mbx.dpcltd-correspondence@mail.mil. The designee should be a General/Flag Officer, a member of the Senior Executive Service, or a Senior Level employee. The designee will work with me in my role as the DoD SAOP, and with their respective privacy programs to continue to strengthen the DoD privacy program.

Responsibilities of SCOPs are outlined in the attachment. To accommodate DoD's organizational structure, SCOPs supporting the Office of the Secretary of Defense (OSD) Principal Staff Assistants have a more limited scope than other DoD Component SCOPs. These differences are noted in the attachment.

I appreciate your support and look forward to continuing to strengthen the DoD privacy program. Questions regarding the SCOP designations and responsibilities should be directed to Ms. Cindy Allard, Chief, DPCLTD, Directorate for Oversight and Compliance, Office of the DCMO, at 703-571-0086 or cindy.l.allard.civ@mail.mil.

CHUNG.JOO.Y.1512306507

Digitally signed by CHUNG.JOO.Y.1512306507
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OSD, cn=CHUNG.JOO.Y.1512306507
Date: 2017.08.28 17:49:10 -04'00'

Joo Y. Chung
Director
DoD Senior Agency Official for Privacy

Attachment:
As stated

ATTACHMENT – Responsibilities of the Senior Component Official for Privacy

The major SCOP responsibilities are listed below. The DoD SAOP has the authority to assign additional responsibilities to the SCOP as needed (e.g., in response to new statutory or regulatory requirements, or changes in policy from OMB).

The following responsibilities apply to all DoD Component SCOPs, including OSD:

- Oversee and provide strategic direction for the respective Component privacy and civil liberties programs.

- Provide advice and information to the DoD SAOP on privacy issues and civil liberties concerns within his or her Component.

- Ensure employee awareness of civil liberties as well as supervisor and senior leader understanding of the responsibility to protect civil liberties in the scope of their authority.

The following responsibilities apply to DoD Component SCOPs, excluding OSD:

- In conjunction with the component security controls assessors and the DoD CIO's Technical Advisory Group:

    - Review and approve, in accordance with the National Institute of Standards and Technology Federal Information Processing Standards Publication 199 and Special Publication 800-60, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

    - Designate which privacy controls will be treated as program management, common, information system-specific, or hybrid privacy controls at the agency.

    - Develop and deploy a process to select and implement privacy controls for information systems and programs that satisfies applicable privacy requirements as stated in OMB guidance.

    - Review and approve the privacy plans portion of the System Security Plan for component information systems before authorization, reauthorization, or ongoing authorization.

    - Identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and management of privacy risks.

    - Identify and maintain inventory of high value assets as defined in OMB Memorandum M-17-09, "Management of Federal High Value Assets."

- Coordinate with authorizing officials on granting Authority to Operate decisions for information systems.

- Ensure that the DoD SAOP is made aware of information systems and components that cannot be appropriately protected or secured, and that the Component ensures such systems are given a high priority for upgrade, replacement, or retirement.

- Implement the DoD breach response plan and, as necessary, establish Component breach management policies, and ensure adequate training and awareness is provided to employees and contractors on how to report and respond to breaches of PII.

- Ensure adequate procedures are in place for the management and remediation of civil liberties complaints.

- Review and approve required reports for submission to the DPCLTD.

- Establish a Component program to provide employee awareness of civil liberties as well as supervisor and senior leader understanding of responsibilities to protect privacy and civil liberties. The program must include and disseminate procedures for submitting and responding to complaints of violations.