highlights. OFOI will redact the document electronically and prepare it for release to the requester.

(6) If OFOI provides the OSD or JS Component with a document for review that was located by another agency, the Component will return the document tasked for review back to OFOI with its release recommendations. The OSD or JS Component will indicate any exempt information with red pencil brackets or electronically.

(7) The FOIA, 5 U.S.C. 552(b) requires the release of segregable information not otherwise exempt. At a minimum, review for segregability shall be at the paragraph level. If OFOI determines that the information is not properly segregated, it will be returned to the OSD or JS Component for further review.

(8) Completed copies of the SD Form 472 and DD Form 2086 shall be returned with the packet. When a denial is based on a security classification according to the criteria outlined in DoD 5200.1–R,[1] the component's decision rationale shall indicate that a current review of the record supports continued classification. The explanation shall also contain the specific rationale from Executive Order 12958 that supports the decision for continued classification of the requested record. All denials of information require the signature of the IDA on the SD Form 472.

(9) A classified document containing unclassified information may not be denied in total under Exemption 1, 5 U.S.C. 552(b)(1), unless the unclassified information, when taken in aggregate, would reveal classified information. This determination must be made in accordance with section 1.7 of Executive Order 12958. Denial of unclassified information not meeting that standard may only be accomplished by exerting one or more of Exemptions 2 through 9 of 5 U.S.C. 552.

(10) All documents, regardless of classification, that are responsive to a FOIA request must be provided to OFOI for processing. This includes Confidential, Secret, Top Secret, and Sensitive Compartmented Information records. OSD and JS Components may contact the OFOI Security Manager to verify OFOI's clearance level for access to classified information.

(11) When an OSD and JS Component cannot locate a requested record and a ''no record'' determination is made, the explanation on the SD Form 472 shall so state and be signed by the IDA. Complete copies of the SD Form 472 and DD Form 2086 shall be returned with the packet.

(c) *Processing FOIA Appeals Within the OSD and JS Components.* (1) When an appeal involves documents denied by an OSD or JS Component IDA, DFOIPO shall review the entire case file of the initial action to determine if the information was properly denied in accordance with 32 CFR part 286 and 5 U.S.C. 552. If the initial action is deemed proper, then DFOIPO will recommend to the appellate authority that the initial action be upheld. When DFOIPO determines that the initial denial should not be upheld on appeal, it shall make a new release recommendation to the OSD or JS Component and return the denied information to OSD or JS Component for its reconsideration. Documents will be processed and returned to OFOI in accordance with the processing procedures outlined in paragraph (b) of this section.

(2) When an appeal involves an initial ''no record'' response, DFOIPO shall review the entire case file to determine if the initial search was adequate. If DFOIPO determines that the administrative record cannot support the adequacy of the initial search, the OSD or JS Component shall be tasked to provide more detailed accounting of the initial search, conduct a new search, or both. If it is determined that the initial administrative record shows that the initial search was adequate, DFOIPO will advise the appellate authority to uphold the original determination.

(3) If the appeal concerns an administrative decision made by DFOIPO such as denial of expedited processing, fee waiver, or a fee category determination, DFOIPO shall review the original case file, along with additional documentary evidence presented by the requester, and make a recommendation to the appellate authority for final adjudication.

(4) When the final determination by DFOIPO involves a full grant, the Chief, FOID or designee shall notify the requester of that determination.

§ 288.7 Information requirements.

The DoD Annual FOIA Report is assigned Report Control Symbol DD–DA&M(A) 1365 in accordance with the requirements of DoD 8910.1–M.[2]

Appendix to Part 288—DoD Agencies and Field Activities, and Other Defense Organizations Served by the Freedom of Information Division

American Forces Information Service
Armed Forces Radiology Research Institute
Defense Acquisition University
Defense Advanced Research Projects Agency
Defense Business Transformation Agency
Defense Equal Opportunity Management Institute
Defense Legal Services Agency
Defense Media Activity
Defense Microelectronics Activity
Defense Modeling and Simulation Office
Defense Prisoner of War/Missing Persons Office
Defense Security Cooperation Agency
Defense Systems Management College
Defense Technology Security Administration
DoD Counterintelligence Field Activity
DoD Human Resources Activity
Joint Professional Military Education Colleges
Missile Defense Agency
National Defense University
Pentagon Force Protection Agency (PFPA)
Uniformed Services University of the Health Sciences
Washington Headquarters Services (WHS)
White House Military Office

September 30, 2008.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. E8–23998 Filed 10–8–08; 8:45 am]

BILLING CODE 5001–06–P

[1] Available at *http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf.*

[2] Available at *http://www.dtic.mil/whs/directives/corres/pdf/891001m.pdf.*

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 325

[DOD–2008–OS–0067]

RIN 0790–AI30

Defense Contract Management Agency (DCMA) Privacy Program

AGENCY: Department of Defense.

ACTION: Proposed rule.

SUMMARY: This part provides policies and procedures for the Defense Contract Management Agency's (DCMA) implementation of a Privacy Program under the Privacy Act of 1974, as amended.

DATES: Comments must be received by December 8, 2008.

ADDRESSES: You may submit comments, identified by docket number and/or RIN number and title, by any of the following methods:

- Federal Rulemaking Portal: *http://www.regulations.gov.* Follow the instructions for submitting comments.
- Mail: Federal Docket Management System Office, 1160 Defense Pentagon, Washington, DC 20301–1160.

Instructions: All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this

Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Debbie Gendreau, (703) 428–1487.

SUPPLEMENTARY INFORMATION:

Executive Order 12866, ''Regulatory Planning and Review''

It has been determined that Privacy Act rules for the Department of Defense are not significant rules. This rule does not (1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a sector of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities; (2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency; (3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or (4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive order.

Public Law 96–354, ''Regulatory Flexibility Act'' (5 U.S.C. Chapter 6)

It has been determined that this Privacy Act rule for the Department of Defense does not have significant economic impact on a substantial number of small entities because it is concerned only with the administration of the Privacy Act within the Department of Defense.

Public Law 95–511, ''Paperwork Reduction Act'' (44 U.S.C. Chapter 35)

It has been determined that this Privacy Act rule for the Department of Defense imposes no information requirements beyond the Department of Defense and that the information collected within the Department of Defense is necessary and consistent with 5 U.S.C. 552a, known as the Privacy Act of 1974.

Section 202, Public Law 104–4, ''Unfunded Mandates Reform Act''

It has been determined that this Privacy Act rulemaking for the Department of Defense does not involve a Federal mandate that may result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100 million or more and that such rulemaking will not significantly or uniquely affect small governments.

Executive Order 13132, ''Federalism''

It has been determined that the Privacy Act rules for the Department of Defense do not have federalism implications. The rule does not have substantial direct effects on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government.

List of Subjects in 32 CFR Part 325

Privacy.

Accordingly 32 CFR Part 325 is added to read as follows:

Sec.

Authority: Privacy Act of 1974, Pub. L. 93–579, Stat. 1896 (5 U.S.C. 552a).

§ 325.1 Purpose and scope.

This part provides policies and procedures for the Defense Contract Management Agency's (DCMA) implementation of a Privacy Program under the Privacy Act of 1974, as amended (5 U.S.C. 552a), OMB Circular A–130,[1] 32 CFR part 310, OMB Memorandum M–07–16,[2] and DoD Policy Memo, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII). [3]

(a) This part applies to all DCMA organizational elements which includes the Headquarters, Divisions, and any Field Activities, and supersedes previously issued guidance on the DCMA Privacy Program.

(b) This part shall be made applicable to DCMA contractors who are operating or maintaining a system of records or portion of a system of records, to include collecting and disseminating records associated with accomplishing the Agency's mission.

[1] Available at *http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf.*

[2] Available at *http://www.whitehouse.gov/omb/memoranda/fy2007/m-16.pdf.*

[3] Available at *http://www.defenselink.mil/privacy/pdfdocs/Safeguarding%20Against%20and%20Responding%20to%20the%20Breach%20of%20PII%20%20-%20OSD%2015041-07.pdf.*

§ 325.2 Definitions.

Agency. For the purpose of disclosing records subject to the Privacy Act among DoD Components, the Department of Defense is considered a single agency. For all other purposes including applications for access and amendment, denial of access or amendment, appeals from denials, and record keeping as regards release to non-DoD agencies, DCMA is considered an agency within the meaning of the Privacy Act.

Government Contractor. The company and its employees who administer or work under a government contract awarded by DCMA. The Contractor and its employees are not considered employees for purposes of FAR 37.104 unless otherwise authorized by statute. However, the Contractor and its employees are considered employees of DCMA for purposes of the criminal provisions of 5 U.S.C. 552a(i) during the performance of the contract whenever a DCMA contract requires the performance of any activities associated with maintaining a system of records subject to the Privacy Act, including the collection, use, and dissemination of records on behalf of the Agency.

Personal Information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her (e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc). Such information also is known as personally identifiable information (e.g., information which can be used to distinguish or trace an individual's identity, such as his or her name; social security number; 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).

§ 325.3 Policy.

It is DCMA policy that:

(a) Individuals have a fundamental right to privacy and the expectation that this Agency, including contractors, will safeguard PII it maintains to the maximum extent practicable.

(1) DCMA shall balance the right of the individual to be protected against unwarranted invasions of personal privacy against agency need when setting any requirement to collect, maintain, use, and disseminate PII, ensuring that such activities are relevant and necessary to achieve a purpose required by statute, Executive Order or regulation.

(2) DCMA personnel, including contractors, have an affirmative responsibility to protect an individual's privacy when collecting, maintaining, using, or disseminating PII.

(3) DCMA shall ensure that policy proposals with potential impact to privacy rights of individuals are evaluated for those impacts and, when required and consistent with the Privacy Provisions of the E-Government Act of 2002 (44 U.S.C. 3501, Note), shall prepare a Privacy Impact Assessment (PIA).

(b) DCMA shall adhere to the rules, regulations, policies, and definitions set forth for implementing a Privacy Act Program by DoD in 32 CFR part 310. DCMA shall create and maintain Privacy Act policy only where it is not already addressed in the authorities listed.

§ 325.4 Responsibilities.

(a) The Director, DCMA, or his/her designee, shall:

(1) Provide adequate funding and personnel to establish and support an effective Privacy Program.

(2) Serve as the Agency Appellate Authority as required under 32 CFR 310.18 and 310.19.

(b) The DCMA Privacy Act Officer, or his/her designee, shall:

(1) Formulate policies, procedures, and standards necessary for uniform compliance with the Privacy Act and 32 CFR part 310 by DCMA activities.

(2) Prepare any Privacy Act Reports as may be mandated by OMB Circular A–130, 32 CFR part 310, and subsequent DoD policy.

(3) Establish and conduct training consistent with the requirements of 32 CFR part 310 for DCMA personnel.

(4) Serve as an Access Denial Authority (ADA) for Headquarters as required under 32 CFR 310.18 and 310.19.

(5) Direct the day-to-day activities of the DCMA Privacy Program.

(6) Coordinate with the DCMA Chief Information Officer (CIO) to formulate procedures and standards for safeguarding against, assessing risk of, handling, reporting, and making proper notification of DCMA PII breaches.

(7) Prepare any required new, amended, or altered system notices for systems of records subject to the Privacy Act and submit them to the Defense Privacy Office for subsequent publication in the **Federal Register**.

(8) Coordinate with DCMA CIO to review PII holdings in accordance with DoD policy.

(9) Develop and maintain a Rules and Consequences policy applicable to all DCMA employees (including managers) and its contractors, licensees, certificate holders and grantees in accordance with DoD policy.

(c) The General Counsel, DCMA, or his/her designee, shall:

(1) Advise and assist the Privacy Act Officer and other DCMA organization Privacy Act Managers as required in the discharge of their responsibilities.

(2) Advise the Defense Privacy Office on the status of DCMA Privacy Act-related litigation.

(3) Consult with DOD General Counsel on final denials, involving issues not able to be resolved within DCMA, or that raise new or significant legal issues of potential significance to other Government agencies.

(4) Coordinate Privacy Act litigation with the Department of Justice.

(5) Coordinate on denials of initial requests and appeals.

(d) The Chief Information Officer, Information Technology, DCMA, or his/her designee, shall:

(1) Formulate and implement protective standards for DCMA PII maintained in automated data processing systems and facilities.

(2) Coordinate with the DCMA Privacy Officer to formulate procedures and standards for safeguarding against, assessing risk of, handling, reporting, and making proper notification of DCMA PII breaches.

(3) Prepare PIAs when required by other authority.

(e) DCMA Division Directors, or their designees, shall:

(1) Assume responsibility for the overall management of the Privacy Act Program within their respective Divisions.

(2) Ensure the Division's internal operating procedures provide for effective compliance with the Privacy Act.

(3) Designate a Privacy Act Manager to serve as the principal point-of-contact on privacy matters.

(4) Serve as an Access Denial Authority for their respective Division. This authority shall not be delegated.

(f) The Division Privacy Act Manager, or his/her designee, shall:

(1) Manage the DCMA Privacy Act Program in accordance with this part and applicable DCMA, DoD, and Federal policies and regulations.

(2) Provide guidelines for managing, administering, and implementing the DCMA Privacy Act Program.

(3) Ensure that the collection, maintenance, use, or dissemination of PII records is in a manner that assures such actions are relevant and necessary for a lawful purpose; that the information is timely, accurate, relevant, and complete for its intended use; and that appropriate safeguards are provided to prevent misuse of such information.

(g) DCMA Procurement Center Officials shall:

(1) Ensure that all contracts awarded by DCMA whose services would subject Government Contractors to the requirements of this part include contractual provisions required by FAR Subpart 24.1 or FAR 39.105.

(2) Ensure that all contracts awarded by DCMA shall require Government Contractor employees to participate in Privacy Act training mandated by DCMA, DoD, or other authority.

(3) Ensure that each contractor covered by this part is contractually required to have its employees sign Certificates of Non-Disclosure prior to being given individual access to DCMA PII (Appendix A to Part 325).

(h) DCMA Military Members and Civilian Employees shall:

(1) Not disclose any PII, except as authorized by this part, DoD or other Federal regulations.

(2) Not maintain any official files which are retrieved by name or other personal identifier without first ensuring a system of records notice has been published in the **Federal Register**.

(3) Participate in Privacy Act training mandated by DCMA, DoD, or other authority.

(4) Report any disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this part to the appropriate Privacy Act officials for action.

(5) Forward to the Division Privacy Act Manager any Privacy Act requests received directly from a member of the public, so that the request may be administratively controlled and processed in accordance with this part.

(6) Adhere to the Standards of Conduct addressed in 32 CFR part 310.

(i) DCMA Contractors shall:

(1) Sign a DCMA Certificate of Non-Disclosure prior to gaining initial access to DCMA PII. (Appendix A to Part 325)

(2) Not disclose any PII, except as authorized by this part.

(3) Not maintain any official files which are retrieved by name or other personal identifier without first ensuring a system of records notice has been published in the **Federal Register**.

(4) Participate in Privacy Act training mandated by DCMA, DoD, or other authority in accordance with their contract.

(5) Report any disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this part to the appropriate Privacy Act officials for action.

(6) Forward to the Division Privacy Act Manager any Privacy Act requests received directly from a member of the public, so that the request may be administratively controlled and processed.

§ 325.5 Procedures.

(a) *Access to records.* (1) Requests for information contained in a DCMA system of records should be addressed to the DCMA Privacy Officer, 6350 Walker Lane, Alexandria, VA 22310. Requests will be processed in accordance with the Privacy Act of 1974 (5 U.S.C. 552a), 32 CFR part 310, the Freedom of Information Act (5 U.S.C. 552), and this part.

(2) *Denial of access.* Access to information contained in a DCMA system of records may be formally denied in accordance with the Privacy Act of 1974 (5 U.S.C. 552a), and 32 CFR part 310.

(b) *Notification when information is lost, stolen, or compromised.* (1) DCMA will respond to breaches in accordance with 32 CFR part 310 as augmented by OMB Memorandum M–07–16, and DoD Policy Memo, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII).

(2) DCMA will establish appropriate administrative, technical, and physical safeguards to protect information against unauthorized disclosure, access or misuse.

(c) *Clauses in DCMA agreements with other government entities.* DCMA will include a DCMA PII Breach Notification Responsibility Statement in all agreements with other government entities that maintain or otherwise have access to DCMA generated personal information. (See Appendix B to Part 325)

Appendix A to Part 325—DCMA Certificate of Non Disclosure

(See section 325.4(h))

NON-DISCLOSURE AGREEMENT

CONTRACT NO. _____

DELIVERY/TASK ORDER NO. _____

I, _____, (hereinafter RECIPIENT), an employee and authorized representative of _____, a Contractor providing support services to the Defense Contract Management Agency (DCMA) with likely access to nonpublic, information, understand and agree to the following:

RECIPIENT is engaged in delivering support services to DCMA under contract; and

It is the intention of DCMA to protect and prevent access to and disclosure of nonpublic sensitive information to anyone other than employees or authorized contractor personnel of the United States Government who have a need to know unless so authorized by the Contracting Officer and/or the Contracting Officer's representative; and

DCMA acknowledges that RECIPIENT will have or require access to such nonpublic information in the course of delivering the contract services; and, finally,

''Nonpublic information'' includes such information as proprietary information (e.g., information submitted by a contractor marked as proprietary), advanced procurement information (e.g., future requirements, statements of work, and acquisition strategies), source selection information (e.g., bids before being made public, source selection plans, and rankings of proposals), trade secrets and other confidential business information (e.g., confidential business information submitted by a contractor), attorney work product, information protected by the Privacy Act (e.g., social security numbers, home addresses and telephone numbers), and other sensitive information that would not be released by DCMA under the Freedom of Information Act (e.g., program, planning and budgeting system information);

RECIPIENT further agrees to and promises as follows:

RECIPIENT shall not seek access to nonpublic information beyond what is required for the performance of the support services contract;

RECIPIENT will ensure that his or her status as a contractor employee is known when seeking access to and receiving such nonpublic information from Government employees;

As to any nonpublic information to which RECIPIENT has or is given access, RECIPIENT shall not use or disclose such information for any purpose other than providing the contract support services, and will not use or disclose the information for any personal or other commercial purpose; and

If RECIPIENT becomes aware of any improper release or disclosure of such nonpublic information, RECIPIENT will advise the contracting officer or a duly authorized representative in writing as soon as possible.

The RECIPIENT agrees to return any nonpublic information given to him or her pursuant to this agreement, including any transcriptions by RECIPIENT of nonpublic information to which RECIPIENT was given access, if not already destroyed, upon RECIPIENT leaving the employ of the contractor providing services to DCMA.

RECIPIENT understands that any unauthorized use, release or disclosure of nonpublic information in violation of this CERTIFICATE, whether during or after leaving the contractor's employ, will subject the RECIPIENT to administrative, civil or criminal remedies as may be authorized by law.

RECIPIENT: _____

(Signature)

DATE: _____

PRINTED NAME: _____

TITLE: _____

Appendix B to Part 325—DCMA PII Breach Notification Responsibility Statement

(See section 325.5(c))

Personally Identifiable Information (PII). In the event *(name of signatory to MOU)* is collecting and maintaining PII on behalf of DCMA and the information is lost, stolen, or otherwise compromised, *(name of signatory to MOU)* shall notify the DCMA Privacy Officer, 6350 Walker Lane, Alexandria, VA 22310, (703) 428–1453, within 24 hours and provide all necessary information regarding the breach. A determination will be made at that time whether DCMA or *(name of signatory to the MOU)* will notify the affected individuals impacted by the breach. *(name of signatory to MOU)* is responsible for filing the Breach notification with US–CERT.

Dated: September 30, 2008.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. E8–23999 Filed 10–8–08; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF THE INTERIOR

National Park Service

36 CFR Part 7

Negotiated Rulemaking Advisory Committee for Off-Road Vehicle Management for Cape Hatteras National Seashore

AGENCY: National Park Service (NPS), Interior.

ACTION: Notice of Meeting Location Change and Additional Public Comment Time for Eighth and Ninth Meetings.

SUMMARY: Notice is hereby given, in accordance with the Federal Advisory Committee Act (Pub. L. 92463, 86 Stat. 770, 5 U.S.C. App 1, section 10), that the meeting location has been changed and an additional public comment time added for the eighth and ninth meeting of the Negotiated Rulemaking Advisory Committee for Off-Road Vehicle (ORV) Management at Cape Hatteras National Seashore. These meetings were noticed on July 8, 2008 at 73 FR 38954. (*See* **DATES** section.)

DATES: The Committee will hold its eighth meeting on November 14–15, 2008, from 8:30 a.m. to 5:30 p.m. on November 14, and from 8:30 a.m. to 4 p.m. on November 15. The meeting on both days will be held at the Wright Brothers National Memorial Pavilion, 1000 Croatan Highway (Milepost 7.6), Kill Devil Hills, North Carolina 25948. The Committee will hold its ninth meeting on December 11–12, 2008, from 8:30 a.m. to 5:30 p.m. on December 11,