also include research and reference material in sufficient quantity to meet curriculum and program demands. Materials shall be, at a minimum, the required readings of the instructor(s) for a particular course or program, or the ability for the student to request a copy of such material, from the institution's main library, without any inconvenience or charge to the student (e.g., a library computer terminal which may allow the student to order material and have it mailed to their residence).

(6) Route locally generated publicity through the base ESO.

(7) Permit employment of off-duty military personnel or Government civilian employees by the institution, provided such employment does not conflict with the policies set forth in DoD Regulation 5500.7–R, "Joint Ethics Regulation." However, Government personnel employed in any way in the administration of this addendum will be excluded from such employment because of conflict of interest.

3. *Billing Procedures, Formal Grades, and Cancellation Provision.*

a. Invoices from institutions must be forwarded to: NETPDTC (Code N8115) Pensacola, FL 32509–5241 within 30 days of course completion.

b. All invoices must have the student name (if more than one name, alphabetically by last name), social security number, course number and description, government cost for each course, and total amount of invoice.

c. All invoices must have an invoice number and date.

d. If the institution has any problems with the billing of an invoice, the institution must notify NETPDTC (Code N8115) Pensacola, FL 32509–5241.

e. Grade reports will be provided to NETPDTC (Code N8115) within 30 days of term ending date or completion of the course, whichever is earlier.

f. Cancellation provision. This addendum may be cancelled by either the Marine Corps or Institution 30 days following the receipt of written notification from the cancelling party.

Appendix E to Part 68—Addendum for Education Services Between [NAME OF EDUCATIONAL INSTITUTION] and the U.S. Navy

1. *Purpose.* This addendum is between (Name of Educational Institution), hereafter referred to as the "Institution," and the United States Navy. The purpose of this agreement is to provide guidelines and procedures for the delivery of educational services to active duty personnel, reservists, eligible retired military personnel, and the Department of Defense (DoD) employees, civilians, and the adult family members not covered in the DoD Voluntary Education Partnership Memorandum Understanding (MOU) between the DoD Office of the Under Secretary of Defense for Personnel and Readiness and the Institution. This addendum is not to be construed in any way as giving rise to a contractual obligation of the Department of the Navy to provide funds to the academic institution that would be contrary to Federal law. This agreement may be amended by the Navy because of changes in statute, executive order, Navy directive, or other federal, state, or local government requirement. Other proposed amendments shall be communicated in writing to the other party, and that party shall have 90 days to provide a written response, and such amendments will only be made upon mutual consent of the parties. This addendum does not extend to any third party contracts between the educational institution and other non-educational institutions.

2. *Responsibilities.*

a. *Commanding Officer responsible for execution of the Voluntary Education program shall:*

(1) Be responsible for determining the local voluntary education program needs for the Navy population to be served and for recommending to the installation commander the educational programs to be offered on the base;

(2) Administer this agreement and provide program management support;

(3) Change Education Services Officer (ESO) to Navy College Office Staff;

(4) Manage the Navy College program Distance Learning Partnership (NCPDLP) agreements.

b. *Navy ESO will:* In support of this addendum, maintain a continuing liaison with the designated Institution representative and be responsible for inspections and the acceptance of the Institution's services. The ESO will provide assistance to the Institution representative to provide military and Navy culture orientation to the Institution personnel.

c. Institution will:

(1) For distance learning partner institution, comply with NCPDLP agreements.

(2) Appoint and designate an Institution Representative to maintain a continuing liaison with the Navy College Office Staff.

(3) Comply with Wide Area Work Flow processes for invoicing of tuition assistance.

(4) Provide a link to the academic institution through the Navy College Program Web Site, only if designated as NCPDLP school.

(5) Display the academic institution's advertising materials (i.e., pamphlets, posters, and brochures) at all Navy College Offices, only if designated as NCPDLP school.

(6) Upon request of the Navy College Office, provide and arrange access to the library and other academic reference and research resources in print or on-line format that are appropriate or necessary to support the courses offered. In addition, these library resource arrangements will be in accordance with the standards of the institution's accrediting association and the State Regulatory Agency having jurisdiction over the academic institution.

(7) Respond to e-mail message from students within one workday. Ensure toll-free telephonic access to academic counseling. Such telephonic access shall be available both in the continental United States and overseas.

(8) Comply with host command procedures before starting instructor-based courses on any Navy installation. The Navy College Office shall negotiate a separate agreement with the academic institution in concert with the host command procedures.

(9) Mail an official transcript indicating degree completion, at no cost to the Sailor or the government to the following address: Navy College Center, VOLED DET N211, Center for Personal and Professional Development, 6490 Saufley Field Road, Pensacola, FL 32509–5204.

d. *Other responsibilities.* Except as otherwise provided in the agreement, any dispute concerning an interpretation of, or a question of fact arising under this agreement which is not disposed of by mutual consent shall be decided by the Commanding Officer CPPD. This decision shall be in writing and constitute the final administrative determination.

e. Cancellation provision. This addendum may be cancelled by either the Navy or Institution 30 days following the receipt of written notification from the cancelling party.

Dated: July 26, 2010.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2010–19314 Filed 8–5–10; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 161

[Docket ID: DOD–2009–OS–0184]

RIN 0790–AI61

Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals

AGENCY: Office of the Under Secretary of Defense for Personnel and Readiness, DoD.

ACTION: Proposed rule.

SUMMARY: The Department of Defense (DoD) proposes to establish policy, assign responsibilities, and provide procedures for the issuing of distinct DoD ID cards. The ID cards shall be issued to uniformed service members, their dependents, and other eligible individuals and will be used as proof of identity and DoD affiliation.

DATES: Comments must be received by October 5, 2010.

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: Chris Fagan at 703–696–0848.

SUPPLEMENTARY INFORMATION:

Regulatory Procedures

Executive Order 12866, "*Regulatory Planning and Review*"

It has been certified that 32 CFR part 161 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 section 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.

Sec. 202, Public Law 104–4, "*Unfunded Mandates Reform Act*"

It has been certified that 32 CFR part 161 does not contain a Federal mandate that may result in expenditure by State, local and Tribal governments, in aggregate, or by the private sector, of $100 million or more in any one year.

Public Law 96–354, "*Regulatory Flexibility Act*" *(5 U.S.C. 601)*

It has been certified that 32 CFR part 161 is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities.

Public Law 96–511, "*Paperwork Reduction Act*" *(44 U.S.C. Chapter 35)*

It has been certified that 32 CFR part 161 does impose reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995.

Executive Order 13132, "*Federalism*"

It has been certified that 32 CFR part 161 does not have federalism implications, as set forth in Executive Order 13132. This rule does not have substantial direct effects on:

(1) The States;

(2) The relationship between the National Government and the States; or

(3) The distribution of power and responsibilities among the various levels of Government.

List of Subjects in 32 CFR Part 161

Administrative practice and procedure, Armed forces, Military personnel, National defense, Privacy, Security measures.

Accordingly, 32 CFR part 161 is proposed to be added to subchapter F to read as follows:

SUBCHAPTER F—SECURITY

PART 161—IDENTIFICATION (ID) CARDS FOR MEMBERS OF THE UNIFORMED SERVICES, THEIR DEPENDENTS, AND OTHER ELIGIBLE INDIVIDUALS

Sec.

Authority: 18 U.S.C. 499, 506, 509, 701, 1001.

PART 161—IDENTIFICATION (ID) CARDS FOR MEMBERS OF THE UNIFORMED SERVICES, THEIR DEPENDENTS, AND OTHER ELIGIBLE INDIVIDUALS

§ 161.1 Purpose.

This part establishes policy, assigns responsibilities, and provides procedures for the issuing of distinct DoD ID cards. The ID cards shall be issued to uniformed service members, their dependents, and other eligible individuals and will be used as proof of identity and DoD affiliation.

§ 161.2 Applicability.

This part applies to:

(a) OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

(b) The Commissioned Corps of the U.S. Public Health Service, under agreement with the Department of Health and Human Services, and the National Oceanic and Atmospheric Administration, under agreement with the Department of Commerce.

§ 161.3 Policy.

It is DoD policy that a distinct DoD ID card shall be issued to uniformed service members, their dependents, and other eligible individuals and will be used as proof of identity and DoD affiliation.

§ 161.4 Responsibilities.

(a) The USD(P&R) shall:

(1) Establish minimum acceptable criteria for establishment and confirmation of personal identity, policy for the issuance of the DoD enterprise personnel identity credentials, and approval of additional systems under the Personnel Identity Protection (PIP) Program in accordance with DoDD 1000.25, "DoD Personnel Identity Protection (PIP) Program" (*see http://www.dtic.mil/whs/directives/corres/pdf/100025p.pdf*).

(2) Act as the Principal Staff Assistant (PSA) for the Defense Enrollment Eligibility Reporting System (DEERS), the Real-Time Automated Personnel Identification System (RAPIDS), and the Personnel Identity Protection (PIP) Program in accordance with DoDD 1000.25.

(3) Maintain the DEERS data system in support of the Department of Defense and applicable legislation and directives.

(4) Develop and field the required RAPIDS infrastructure and all elements of field support to issue ID cards including but not limited to software distribution, hardware procurement and installation, on-site and depot-level hardware maintenance, on-site and Web-based user training and central telephone center support, and telecommunications engineering and network control center assistance.

(5) In coordination with the Under Secretary of Defense for Intelligence (USD(I)), Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO), and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), establish policy and oversight for common access card (CAC) life-cycle compliance with Federal Information Processing Standards (FIPS) Publication 201–1, "Personal Identity Verification (PIV) of Federal Employees and Contractors" (*http://csrc.nist.gov/*

publications/fips/fips201-1/FIPS-201-1-chng1.pdf).

(b) The Assistant Secretary of Defense for Health Affairs (ASD(HA)), under the authority, direction, and control of the USD(P&R), shall develop overall policy and establish procedures for providing medical care through the Military Health System to authorized beneficiaries and eliminate fraud, waste, and abuse in the provision of medical benefits.

(c) The Assistant Secretary of Defense for Reserve Affairs (ASD(RA)), under the authority, direction, and control of the USD(P&R), shall develop policies and establish guidance for the National Guard and Reserve Component communities that impact benefits, entitlements, identity, and ID cards.

(d) The Deputy Under Secretary of Defense for Military Community and Family Policy (DUSD(MC&FP)), under the authority, direction, and control of the USD(P&R), shall develop policy and procedures to determine eligibility for access to DoD programs for morale, welfare, and recreation; commissaries; exchanges; lodging; children and youth; DoD schools; family support; voluntary and post-secondary education; and other military community and family benefits that impact identity and ID cards.

(e) The Director, Defense Human Resources Activity, under the authority, direction, and control of the USD(P&R), shall, in accordance with DoDD 1000.25:

(1) Develop policies and procedures for the oversight, funding, personnel staffing, direction, and functional management of the PIP Program.

(2) Coordinate with the Principal Deputy Under Secretary of Defense for Personnel and Readiness, the ASD(HA), and the ASD(RA) on changes to enrollment and eligibility policy and procedures pertaining to personnel, medical, and dental issues that impact the PIP Program.

(3) Develop policies and procedures to support the functional requirements of the PIP Program, DEERS, and the DEERS client applications.

(4) Secure funding in support of new requirements to support the PIP Program or the enrollment and eligibility functions of DEERS and RAPIDS.

(5) Approve the addition or elimination of population categories eligible for ID cards in accordance with applicable law.

(6) Establish the type and form of ID card issued to eligible population categories and administer pilot programs to determine the suitable form of ID card for newly identified populations.

(f) The USD(AT&L) shall:

(1) Issue regulatory coverage for CAC and Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors" (see *http://www.cac.mil/assets/pdfs/HSPD_12.pdf*) for contracts.

(2) Communicate Homeland Security Presidential Directive 12 requirements to the DoD acquisition community.

(3) Ensure that the requirement for contractors to return CACs at the completion or termination of each individual's support on a specific contract is included in all applicable contracts.

(g) The USD(I) shall:

(1) Establish policy for the use of ID cards for physical access purposes in accordance with DoD 5200.08–R.

(2) Establish policy for military, civilian, and contractor employee background investigation, submission, and adjudication across the Department of Defense, in compliance with Homeland Security Presidential Directive 12 and in accordance with DoD 5200.2–R.

(h) The ASD(NII)/DoD CIO shall:

(1) In coordination with the USD(I), USD(P&R), and USD(AT&L), establish policy and oversight for CAC life-cycle compliance with FIPS Publication 201–1.

(2) Provide guidance to DoD information systems administrators regarding use of non-DoD identification credentials, including the Federal PIV cards, for authenticating to DoD network accounts and DoD private Web sites.

(3) Ensure that the DoD public key infrastructure conforms to all applicable FIPS to the greatest extent possible.

(i) The Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA)), under the authority, direction, and control of the Under Secretary for Policy (USD(P)), shall facilitate force protection activities with the law enforcement community.

(j) The Heads of the DoD Components, the Director, USPHS, and the Director, NOAA shall:

(1) Develop and implement Component-level procedures for DoD directed policies or legislative requirements to support benefits eligibility through DEERS.

(2) Develop and implement Component-level ID card life-cycle procedures to comply with the provisions of this part.

(3) Ensure all DoD employees, Military Service members, and all other eligible CAC applicants, to include contract support and other affiliate CAC applicants, have met the background investigation requirements in paragraph (b)(3) of this section prior to approving CAC sponsorship and registration. Background investigation status must be verified and documented by the sponsor or sponsoring organization in conjunction with application for CAC issuance.

(4) Establish processes and procedures as part of the normal check-in and check-out process for collection of the CAC for all categories of DoD personnel when there is a separation, retirement, termination, contract termination or expiration, or CAC revocation. Since CACs contain personally identifiable information (PII), they shall be treated and controlled in accordance with DoD 5400.11–R, "Department of Defense Privacy Program" (*see http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf*) and DoD 5200.1–R, "Information Security Program" (*see http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf*). These cards shall be returned to any RAPIDS issuance location for proper disposal in a timely manner once surrendered by the CAC holder.

(5) Provide appropriate space and staffing for ID card issuing operations, as well as reliable telecommunications to and from the Defense Information Systems Agency managed Non-Secure Internet Protocol Router Network.

(6) Provide funding for CAC cardstock, printer consumables, and electromagnetically opaque sleeves to Defense Manpower Data Center (DMDC).

(7) Protect cardstock and consumables in accordance with the guidelines and standards maintained by DMDC.

(8) In accordance with FIPS Publication 201–1, provide electromagnetic opaque sleeves or other comparable technologies to protect against any unauthorized contactless access to the cardholder unique identification number stored on the CAC.

(9) Manage the distribution and locations of DoD Component-specific CAC personal identification number (PIN) reset workstations.

(10) To the maximum extent possible, and in accordance with DoD Components' designated approving authority guidelines, ensure networked workstations are properly configured and available for CAC holders to use the User Maintenance Portal-Post Issuance Portal service.

(11) Oversee supervision of Contractor Verification System trusted agents (TAs) and trusted agent security managers and ensure the number of contractors overseen by any TA is manageable.

§ 161.5 Procedures.

(a) *ID cards.* (1) DoD ID cards shall serve as the Geneva Convention Card for eligible personnel in accordance with DoDI 1000.1, "Identity Cards Required by the Geneva Conventions" (*http://www.dtic.mil/whs/directives/corres/pdf/100001p.pdf*).

(2) DoD ID cards shall be issued through a secure and authoritative process to ensure that access to DoD physical and logical assets is granted based on authenticated and secure identity information in accordance with DoDD 1000.25.

(3) The CAC, a form of DoD ID card, shall serve as the Federal PIV card for DoD implementation of Homeland Security Presidential Directive 12.

(4) ID cards, in a form distinct from the CAC, shall be issued and will serve as proof of identity and DoD affiliation for eligible communities that do not require the Federal PIV card that complies with FIPS Publication 201–1 and Homeland Security Presidential Directive 12.

(b) *ID card life cycle.* The ID card life cycle shall be supported by an infrastructure that is predicated on a systems-based model for credentialing as described in FIPS Publication 201–1. Paragraphs (b)(1) through (7) of this section represent the baseline requirements for the ID card life cycle. The specific procedures and sequence of order for these items will vary based on the applicant's employment status or affiliation with the Department of Defense and the type of ID card issued. Detailed procedures of the ID card life cycle for each category of applicant and type of ID card shall be provided by the responsible agency.

(1) *Sponsorship and eligibility.* Sponsorship shall incorporate the processes for confirming eligibility for an ID card. The sponsor is the person affiliated with the Department of Defense or other Federal agency who takes responsibility for verifying and authorizing the applicant's need for an ID card. Applicants for a CAC must be sponsored by a government official or employee.

(2) *Registration and enrollment.* Sponsorship and enrollment information on the ID card applicant shall be registered in DEERS prior to card issuance.

(3) *Background investigation.* A background investigation is required for those individuals eligible for a CAC. A background investigation is not currently required for those eligible for other forms of DoD ID cards. Sponsored CAC applicants shall not be issued a CAC without the required background investigation stipulated in Federal Information Processing Standards Publication 201–1. Applicants that have been denied a CAC based on an unfavorable adjudication of the background investigation may submit an appeal in accordance with DoD 5200.2–R.

(4) *Identity and eligibility verification.* Identity and eligibility verification shall be completed at a RAPIDS workstation. Verifying Officials (VOs) shall inspect identity and eligibility documentation and RAPIDS shall authenticate individuals to ensure that ID cards are provided only to those sponsored and with a current affiliation with the Department of Defense. RAPIDS shall also capture uniquely identifying characteristics that bind an individual to the information maintained on that individual in DEERS and to the ID card issued by RAPIDS. These characteristics may include, but are not limited to, digital photographs and fingerprints.

(5) *Issuance.* ID cards shall be issued at the RAPIDS workstation after all sponsorship, enrollment and registration, background investigation (CAC only), and identity and eligibility verification requirements have been satisfied.

(6) *Use and maintenance.* ID cards shall be used as proof of identity and DoD affiliation to facilitate access to DoD facilities and systems. Additionally, ID cards shall represent authorization for entitled benefits and privileges in accordance with DoD policies.

(7) *Retrieval and revocation.* ID cards shall be retrieved by the sponsor or sponsoring organization when the ID card has expired, when it is damaged or compromised, or when the card holder is no longer affiliated with the Department of Defense or no longer meets the eligibility requirements for the card. The active status of an ID card shall be revoked within the DEERS and RAPIDS infrastructure and, for CAC, the PKI certificates on the CAC shall be revoked.

(c) *Guidelines and restrictions.* The guidelines and restrictions in this paragraph (c) apply to all forms of DoD ID cards.

(1) Any person willfully altering, damaging, lending, counterfeiting, or using these cards in any unauthorized manner is subject to fine or imprisonment or both, as prescribed in 18 U.S.C. 499, 506, 509, 701, and 1001. Section 701 prohibits photographing or otherwise reproducing or possessing DoD ID cards in an unauthorized manner, under penalty of fine or imprisonment or both. Unauthorized or fraudulent use of ID cards would exist if bearers used the card to obtain benefits and privileges to which they are not entitled. Photocopying of DoD ID cards to facilitate medical care processing, check cashing, voting, tax matters, the Servicemember's Civil Relief Act, or administering other military-related benefits to eligible beneficiaries are examples of authorized photocopying. When possible, the ID card will be electronically authenticated in lieu of photographing the card.

(2) Treaties, status-of-forces agreements (SOFAs), or military base agreements in overseas areas may place limitations on the logistical support that otherwise might be available to eligible personnel. SOFAs with foreign countries may limit the use of commissary or exchange facilities to persons who are stationed or performing temporary duty with the host nation under official orders in support of the mutual defense mission. ID cards shall not be issued for the sole purpose of implementing restrictions under SOFAs. ID cards shall be issued in accordance with this part and the uniformed services shall use other means, such as ration cards, to implement restrictions under SOFAs as required.

(3) All ID cards are property of the U.S. Government and shall be returned upon separation, resignation, firing, termination of contract or affiliation with the Department of Defense, or upon any other event in which the individual no longer requires the use of such ID card.

(4) ID cards that are expired, invalidated, stolen, lost, or otherwise suspected of potential or actual unauthorized use shall have the status of the cards revoked in DEERS and, for CACs, have the PKI certificates immediately revoked to prevent any unauthorized use.

(5) There are instances where graphical representations of ID cards are necessary to facilitate the DoD mission. When used and/or distributed, the replicas must not be the same size as the ID card, must have the word "SAMPLE" written on them, and shall not contain an individual's PII. All sample ID cards must be maintained in a controlled environment and shall not serve as a valid ID.

(6) Individuals within the Department of Defense who have multiple personnel category codes (*e.g.,* an individual who is both a reservist and a contractor) shall be issued a separate ID card in each personnel category for which they are eligible. Multiple current ID cards of the same form (*e.g.,* CAC) shall not be issued or exist for an individual under a single personnel category code.

(7) ID cards shall not be amended, modified, or overprinted by any means.

No stickers or other adhesive materials are to be placed on either side of an ID card. Holes shall not be punched into ID cards, except when a CAC has been requested by the next of kin for an individual who has perished in the line of duty. A CAC provided to next of kin shall have the status of the card revoked in DEERS, have the certificates revoked, and have a hole punched through the integrated circuit chip prior to release of the CAC to the next of kin.

(8) An ID card shall be in the personal custody of the individual to whom it was issued at all times. If required by military authority, it shall be surrendered for ID or investigation.

(d) *CAC migration to Federal PIV requirements.* The Department of Defense is currently migrating the CAC to meet the Federal requirements for credentialing contained within FIPS Publication 201–1 and Homeland Security Presidential Directive 12. Migration will take place over multiple years as the card issuance hardware, software, and supporting systems and processes are upgraded. Successful migration will require coordination and collaboration within and among all CAC communities (*e.g.,* personnel security, operational security, industrial security, information security, physical security, and information technology). The following organizations will support the migration in conjunction with the responsibilities listed in § 161.3:

(1) The DMDC shall:

(i) Procure and distribute CAC consumables, including card stock, electromagnetically opaque sleeves, and printer supplies, commensurate with funding received from the DoD Components.

(ii) In coordination with the Office of the Under Secretary of Defense for Policy (OUSD(P)), establish an electronic process for securing CAC eligibility information on foreign government military, employee, or contract support personnel whose visit status and background investigation has been confirmed, documented, and processed by OUSD(P) according to DoDD 5230.20 (*see http://www.dtic.mil/whs/directives/corres/pdf/523020p.pdf*).

(iii) In accordance with DoD Directive 5400.11, electronically capture and store source documents in the identity proofing process at the accession points for eligible ID card holders

(iv) Implement modifications to the CAC applets and interfaces, add contactless capability to the CAC platform, and, in accordance with DoD 5400.11–R, implement modifications to the CAC topology to support compliance with FIPS Publication 201–1.

(v) Establish and implement procedures for capturing biometrics required to support CAC issuance, which includes fingerprints and facial images specified in FIPS Publication 201–1 and National Institute of Standards and Technology Special Publication 800–76–1, "Biometric Data Specification for Personal Identity Verification" (*see http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf*).

(vi) In coordination with the Executive Manager for DoD Biometrics and the Office of the USD(AT&L), implement the capability to obtain two segmented images (primary and secondary) fingerprint minutia from the full 10-print fingerprints captured as part of the initial background investigation process for CAC issuance.

(vii) Maintain a capability for a CAC holder to reset or unlock PINs from a system outside of the CAC issuance infrastructure.

(2) The Executive Manager for DoD Biometrics shall:

(i) Establish biometric standards for the collection, storage, capture, and subsequent transmittal of biometric information in accordance with DoDD 8521.01E, "Department of Defense Biometrics" (*see http://www.dtic.mil/whs/directives/corres/pdf/852101p.pdf*).

(ii) In coordination with the Offices of the USD(P&R) and USD(I) and the DoD Components, establish capability for biometric capture and enrollment operations to support CAC issuance in accordance with DoD 5400.11–R and National Institute of Standards and Technology Special Publication 800–76–1.

(3) The Identity Protection and Management Senior Coordinating Group shall:

(i) Monitor the CAC and identity management related activities outlined within this part in accordance with DoDD 1000.25.

(ii) Maintain a configuration management process for the CAC and its related components to monitor DoD compliance with FIPS Publication 201–1.

Dated: July 26, 2010.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2010–19315 Filed 8–5–10; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 199

[DOD–2010–HA–0033]

RIN 0720–AB44

TRICARE: Unfortunate Sequelae From Noncovered Services in a Military Treatment Facility

AGENCY: Office of the Secretary, Department of Defense.

ACTION: Proposed rule.

SUMMARY: The Department of Defense is publishing this proposed rule to allow coverage for otherwise covered services and supplies required in the treatment of complications (unfortunate sequelae) resulting from a noncovered incident of treatment provided in a Military Treatment Facility (MTF), when the initial noncovered service has been authorized by the MTF Commander and the MTF is unable to provide the necessary treatment of the complications. This proposed rule is necessary to protect TRICARE beneficiaries from incurring financial hardships due to the current regulatory restrictions that prohibit TRICARE coverage of treatment of the complications resulting from noncovered medical procedures, even when those procedures were conducted in a Department of Defense facility.

DATES: Comments received at the address indicated below by October 5, 2010 will be accepted.

ADDRESSES: You may submit comments, identified by docket number and/or Regulatory Information Number (RIN) and title, by either 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 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: René Morrell, Medical Benefits and Reimbursement Branch, TRICARE Management Activity, (303) 676–3618.