**Billing Code: 5001-06**

**DEPARTMENT OF DEFENSE**

**Office of the Secretary**

**32 CFR Part 221**

**[Docket ID: DOD-2015-OS-0054]**

**RIN 0790-AJ36**

**DoD Identity Management**

**AGENCY:** Under Secretary of Defense for Personnel and Readiness (USD(P&R)), DoD.

**ACTION:** Proposed rule.

**SUMMARY:** This rulemaking establishes implementation guidelines for DS Logon to provide a secure means of authentication to applications containing personally identifiable information (PII) and personal health information (PHI). This will allow beneficiaries and other individuals with a continuing affiliation with DoD to update pay or health-care information in a secure environment. This service can be accessed by active duty, National Guard and Reserve, and Commissioned Corps members of the uniformed services when separating from active duty or from the uniformed service.

**DATES:** Comments must be received by **[INSERT DATE 60 DAYS FROM THE DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

**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: Department of Defense, Office of the Deputy Chief Management Officer, Directorate for Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Alexandria, VA 22350-1700.

*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:** Mr. Robert Eves, Defense Human Resources Activity, 571-372-1956.

**SUPPLEMENTARY INFORMATION:**

**Background**

This proposed rule describes procedures for obtaining a DS Logon credential for all active duty, National Guard and Reserve, and Commissioned Corps members of the uniformed services when separating from active duty or from the uniformed service. It discusses how credential holders may maintain and update their credentials and manage their personal settings. Finally, it discusses the permissions credential holders have to access their information, who has access to view and edit their information, and who is eligible to act on their behalf.

DoD collects and maintains information on Service members, beneficiaries, DoD employees, and other individuals affiliated with the DoD in order to issue DoD identification (ID) cards that facilitate access to DoD benefits, DoD installations, and DoD information systems. This action formally establishes DoD policy requirements for DoD Self-Service (DS) Logon credentials that are used to facilitate logical access to self-service websites. This regulatory action will update the

CFR for DoD Manual (DoDM) 1341.02, volume 1, "DoD Identity Management: DoD Self-Service (DS) Logon Program and Credential.

**Authorities**

The DoD PIP Program uses emerging technologies to support the protection of individual identity and to assist with safeguarding DoD physical assets, networks, and systems from unauthorized access based on fraudulent or fraudulently obtained credentials. DEERS is the authoritative data source for identity and verification of affiliation with the DoD in accordance with the DoD PIP Program. Specific authorities are listed below.

- Title 10 U.S.C. 1044a. This section establishes the authority for a Judge Advocate, other member of the armed forces, designated by law and regulations, or other eligible persons to have the powers to act as a notary. The persons identified in Title 10 U.S.C 1044a subsection (b) have the general power of a notary and may notarize a completed and signed DD Form 3005, "Application for Surrogate Association for DoD Self-Service (DS) Logon."
- DoD Instruction 1000.25, "DoD Personnel Identity Protection (PIP) Program" (available at http://www.dtic.mil/whs/directives/corres/pdf/100025p.pdf). This issuance establishes minimum acceptable criteria for the establishment and confirmation of personal identity and for the issuance of DoD personnel identity verification credentials.
- DoD Instruction 1341.2, "Defense Enrollment Eligibility Reporting System (DEERS) Procedures" (available at http://www.dtic.mil/whs/directives/corres/pdf/134102p.pdf). This issuance establishes DEERS as the authoritative data source for identity and verification of affiliation with the DoD, and benefit eligibility to include medical, dental, and pharmacy.

- Office of Management and Budget M-04-04, "E-Authentication Guidance for Federal Agencies" (available at www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf). This memorandum requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance, establishing and describing four levels of identity assurance for electronic transactions requiring authentication.
- 32 CFR part 310. This CFR part established the DoD Privacy Program in accordance with the provisions of the Privacy Act of 1974, and prescribes uniform procedures for the implementation of and compliance with the DoD Privacy Program

**Costs And Benefits Of This Regulatory Action**

The annual operating costs for the DS Logon program are approximately $1,265,305.35. Based on 6 million active users, the cost per user is about $0.21. The benefits include extending a secure means of authentication to PII and PHI to all DoD beneficiaries and other individuals with a continuing affiliation with DoD who previously had no logical access. Only one DS Logon credential may exist for an individual eliminating separate username/password combinations for each application to be accessed, allowing users to better manage their means of authentication to DoD information systems. The DS Logon credentials are credentialed at National Institute of Standards and Technology (NIST) e-authentication levels 1, 2, and 3, in accordance with NIST Special Publication 800-63-2 (available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf), and at Credential Strength A and B, in accordance with DoDI 8520.03 (available at: http://www.dtic.mil/whs/directives/corres/pdf/852003.pdf, meeting the required sensitivity level for access to self-service personal information.

**Regulatory Procedures**

Executive Order 12866, "Regulatory Planning and Review" and Executive Order 13563, "Improving Regulation and Regulatory Review"

Executive Orders 13563 and 12866 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distribute impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a "significant regulatory action," although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the proposed rule has been reviewed by the Office of Management and Budget (OMB).

Section 202, Public Law 104-4, "Unfunded Mandates Reform Act"

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) (Pub. L. 104-4) requires agencies assess anticipated costs and benefits before issuing any rule whose mandates require spending in any 1 year of $100 million in 1995 dollars, updated annually for inflation. In 2014, that threshold is approximately $141 million. This proposed rule would not mandate any requirements for State, local, or tribal governments, nor will it affect private sector costs.

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

The Department of Defense certifies that this proposed rule 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. Therefore, the Regulatory Flexibility Act, as amended, does not require us to prepare a regulatory flexibility analysis.

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

Section 221.6(d)(2)(i)(A) of this proposed rule contains information collection requirements. DoD has submitted the following proposal to OMB under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35). Comments are invited on: (1) whether the proposed collection of information is necessary for the proper performance of the functions of DoD, including whether the information will have practical utility; (2) the accuracy of the estimate of the burden of the proposed information collection; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the information collection on respondents, including the use of automated collection techniques or other forms of information technology.

Title: Application for Surrogate Association for DoD Self-Service (DS) Logon.

Type of Request: New

Number of Respondents: 5,000

Responses Per Respondent: 1

Annual Responses: 5,000

Average Burden Per Response: 2 minutes.

Annual Burden Hours: 167 hours

Needs and Uses: This information collection is consistent with Department of Defense (DoD) guidelines that have been outlined in draft DoD Manual (DoDM) 1341.02, volume 1, "DoD Identity Management: DoD Self-Service (DS) Logon Program and Credential," which authorizes Defense Enrollment Eligibility Reporting System (DEERS) enrollment and DS Logon credential issuance to surrogates. A surrogate may be established as the custodian of a deceased Service member's unmarried minor child(ren) who is under 18, who is at least 18 but under 23

and attending school full-time, or who is incapacitated. A surrogate may also be established as the agent of an incapacitated dependent (e.g., spouse, parent) or of a wounded, ill, or incapacitated Service member.

This information collection is needed to obtain the necessary data to establish eligibility for a DS Logon credential and enrollment in DEERS.

This information shall be used to establish an individual's eligibility for DEERS enrollment and DS Logon credential issuance as a surrogate. Once this information has been collected, a record will be established in DEERS and a DS Logon credential issued in accordance with DoDM 1341.02, volume 1. The information that is collected may be released to Federal and State agencies and private entities, on matters relating to utilization review, professional quality assurance, program integrity, civil and criminal litigation, and access to Federal government facilities, computer systems, networks, and controlled areas.

Affected Public: 5,000

Frequency: On occasion.

Respondent's Obligation: Required to obtain DEERS enrollment and a DS Logon credential as a surrogate.

OMB Desk Officer: Jasmeet Seehra.

Written comments and recommendations on the proposed information collection should be sent to Jasmeet Seehra at Oira_submission@omb.eop.gov, with a copy to the Defense Human Resources Activity, Suite 06J25, 4800 Mark Center Drive, Alexandria, Virginia, 22350-4000. Comments can be received from 30 to 60 days after the date of publication of this proposed rule, but comments to OMB will be most useful if received by OMB within 30 days after the date of publication of this proposed rule.

You may also submit comments, identified by docket number and title, by the following method:

* Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name, docket number and title 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.

To request more information on this proposed information collection or to obtain a copy of the proposal and associated collection instruments, please write to Defense Human Resources Activity, Suite 06J25, 4800 Mark Center Drive, Alexandria, Virginia, 22350-4000; Mr. Robert Eves; 571-372-1956.

Executive Order 13132, "Federalism"

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has Federalism implications. This proposed rule will not have a substantial effect on State and local governments.

**List of Subjects in 32 CFR Part 221**

Identity management, Identification cards, Logon credentials.

Accordingly, 32 CFR part 221 is proposed to be added to read as follows:

**PART 221—DOD IDENTITY MANAGEMENT**

Sec.
221.1 Purpose.
221.2 Applicability.
221.3 Definitions.
221.4 Policy.
221.5 Responsibilities.
221.6 Procedures.

Authority: 10 U.S.C. 1044a.

**§ 221.1 Purpose.**

(a) The purpose of the overall part is to implement policy, assign responsibilities, and provide procedures for DoD personnel identification.

(b) This part establishes implementation guidelines for DS Logon.

**§ 221.2 Applicability.**

This part applies to:

(a) The Office of the Secretary, 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 DoD (referred to collectively in this part as the "DoD Components").

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

**§ 221.3 Definitions.**

Unless otherwise noted, the following terms and their definitions are for the purposes of this part:

Beneficiary. Individuals affiliated with the DoD that may be eligible for benefits or entitlements.

Certified copy. A copy of a document that is certified as a true original and:

(1) Conveys the appropriate seal or markings of the issuer;

(2) Has a means to validate the authenticity of the document by a reference or source number;

(3) Is a notarized legal document or other document approved by a judge advocate, member of any of the armed forces, or other eligible person in accordance with 10 U.S.C. 1044a; or

(4) Has the appropriate certificate of authentication by a U.S. Consular Officer in the foreign country of issuance which attests to the authenticity of the signature and seal.

DoD beneficiary (DB). Beneficiaries who qualify for DoD benefits or entitlements in accordance with National Institute of Science and Technology Special Publication 800-63-2, "Electronic Authentication Guideline" (available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf). This population may include widows, widowers, and eligible former spouses.

Dependent. An individual whose relationship to the sponsor leads to entitlement to benefits and privileges.

DS Logon credential. A username and password to allow Service members, beneficiaries, and other individuals affiliated with the DoD secure access to self-service websites.

DS Logon credential holder. A Service member, beneficiary, and other individual affiliated with the DoD who has applied for and received a DS Logon credential

Former member. An individual who is eligible for, or entitled to, retired pay for non-regular service in accordance with 31 U.S.C. chapter 1223, but who has been discharged from the Service and who maintains no military affiliation.

Former spouse. An individual who was married to a uniformed services member for at least 20 years, and the member had at least 20 years of service creditable toward retirement, and the marriage overlapped as follows:

(1) Twenty years marriage, 20 years creditable service for retirement, and 20 years overlap between the marriage and the service (referred to as 20/20/20). The benefits eligibility begins on the date of divorce;

(2) Twenty years marriage, 20 years creditable service for retirement, and 15 years overlap between the marriage and the service (referred to as 20/20/15). The benefits eligibility begins on the date of divorce; or

(3) A spouse whose marriage was terminated from a uniformed service member who has their eligibility to receive retired pay terminated as a result of misconduct based on Service-documented abuse of the spouse and has 10 years of marriage, 20 years of creditable service for retirement, 10 years of overlap between the marriage and the service (referred to as 10/20/10). The benefits eligibility begins on the date of divorce.

Legal guardian (LG). The terms "guardian" and "conservator" are used synonymously. Some States may limit the authority of a guardian to specific types of health care decisions; a court may also impose limitations on the health care decisions.

Surrogate. A person who has been delegated authority, either by an eligible individual who is at least 18 years of age and mentally competent to consent or by a court of competent

jurisdiction in the United States (or possession of the United States), to act on behalf of the eligible individual in a specific role.

Widow. The female spouse of a deceased member of the uniformed services.

Widower. The male spouse of a deceased member of the uniformed services.

**§ 221.4 Policy.**

In accordance with DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program" (available at http://www.dtic.mil/whs/directives/corres/pdf/100025p.pdf), DoD Instruction 1341.2, "Defense Enrollment Eligibility Reporting System (DEERS) Procedures" (available at http://www.dtic.mil/whs/directives/corres/pdf/134102p.pdf), Office of Management and Budget M-04-04, "E-Authentication Guidance for Federal Agencies" (available at www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf) and 32 CFR part 310, it is DoD policy that DoD will provide a secure means of authentication to PII and personal health information (PHI) for all beneficiaries and other individuals with a continuing affiliation with DoD.

**§ 221.5 Responsibilities.**

(a) The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) oversees implementation of the procedures within this part.

(b) Under the authority, direction, and control of the USD(P&R), and in addition to the responsibilities in paragraph (c) of this section, the Director, DoDHRA, through the Director, DMDC:

(1) Approves the addition or elimination of population categories for DS Logon eligibility.

(2) Develops and fields the required Defense Enrollment Eligibility Reporting System (DEERS) and RAPIDS infrastructure and all elements of field support required to support the

management of the DS Logon credential including, but not limited to, issuance, storage, maintenance, and customer service.

(3) Obtains and distributes DS Logon credentials, and provides a secure means for delivery.

(c) The DoD Component heads:

(1) Comply with this part and distribute this guidance to applicable stakeholders.

(2) Provide manpower for issuance of DS Logon credentials and instruction for use to all eligible individuals who are requesting a DS Logon credential in conjunction with the issuance of a DoD identification (ID) card or who are applying for a DS Logon credential as a surrogate, when responsible for a DoD ID card site(s).

(d) The Secretaries of the Military Departments, in addition to the responsibilities in paragraph (c) of this section, and the heads of the non-DoD uniformed services:

(1) Comply with this part and distribute this guidance to applicable stakeholders.

(2) Provide manpower for issuance of DS Logon credentials and instruction for use to all eligible individuals who are requesting a DS Logon credential in conjunction with the issuance of a DoD ID card or who are applying for a DS Logon credential as a surrogate.

(3) Ensure all Active Duty, National Guard and Reserve, and Commissioned Corps members of their uniformed services obtain a DS Logon credential when separating from active duty or from the uniformed service.

**§ 221.6 Procedures.**

(a) General. A DS Logon credential will be made available to all beneficiaries that are eligible for DoD-related benefits or entitlements to facilitate secure authentication to critical websites. This includes members of the uniformed services, veterans with a continuing

affiliation to the DoD, spouses, dependent children aged 18 and over, and other eligible individuals identified in paragraph (b) of this section.

(b) Overview. Only one DS Logon credential may exist for an individual, regardless of the number of affiliations an individual may have to the DoD.

(1) Eligibility. Beneficiaries of DoD-related benefits or entitlements and other individuals with a continuing affiliation with the DoD may be eligible for a DS Logon credential. Eligible populations include:

(i) Veterans, including former members, retirees, Medal of Honor recipients, disabled American veterans, and other veterans with a continuing affiliation to the DoD.

(ii) Retired DoD civilian employees, including retired NOAA Wage Mariners.

(iii) Eligible dependents in accordance with volume 2 of DoD Manual 1000.13, "DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals" (available at http://www.dtic.mil/whs/directives/corres/pdf/100013_vol2.pdf), including spouses, dependent children aged 18 or older, and dependent parents.

(iv) DBs, including eligible widows, widowers, and former spouses, in accordance with volume 2 of DoD Manual 1000.13.

(v) Surrogates, as described in paragraph (d) of this section.

(vi) Other populations as determined by the Director, DMDC.

(c) Lifecycle—(1) Application. Eligible individuals, as identified in paragraph (b)(1) of this section, may apply for a DS Logon credential:

(i) Online. Individuals with Internet access may apply for a sponsor or dependent DS Logon by submitting a:

(A) My Access Center website request. This type of request supports the provisioning of a Basic DS Logon credential. The My Access Center website can be accessed at https://myaccess.dmdc.osd.mil/.

(B) CAC request. Individuals with a CAC, a computer with Internet access and a CAC reader may apply for either a sponsor or a dependent DS Logon credential via the My Access Center website or any application that has implemented DS Logon.

(1) A sponsor DS Logon credential is provisioned immediately upon request. This type of request supports the provisioning of a Premium DS Logon credential.

(2) A request for a DS Logon credential on behalf of a dependent generates an activation letter with an activation code that is mailed to the sponsor at his or her home address in DEERS. Once complete, this type of request supports the provisioning of a Premium DS Logon credential.

(C) Request using a Defense Finance and Accounting Services (DFAS) myPay account. Eligible individuals may apply for a sponsor or dependent DS Logon credential using a DFAS myPay personal identification number via the My Access Center website. A request for a DS Logon credential generates an activation letter with an activation code that is mailed to the sponsor at his or her home address in DEERS. Once complete, this type of request supports the provisioning of a Premium DS Logon credential.

(ii) Via remote proofing. Eligible individuals with an existing DEERS record may apply for a sponsor or dependent DS Logon credential using remote proofing via the My Access Center website. Individuals requesting a DS Logon credential via remote proofing must correctly answer a number of system-generated questions. Once remote proofing is completed, a Premium DS Logon credential is provisioned immediately.

(iii) Via in-person proofing. Eligible individuals may apply for a sponsor or dependent DS Logon credential using in-person proofing. In-person proofing is performed at Department of Veterans Affairs regional offices where the DS access station application is implemented, and at DoD ID card sites when a DS Logon credential is requested either in conjunction with DoD ID card issuance or during initial enrollment of a surrogate. Once in-person proofing is completed, a Premium DS Logon credential is provisioned immediately. Individuals requesting a DS Logon credential via in-person proofing must present:

(A) Identity documents. DS Logon credential applicants must satisfy the identity verification criteria in paragraph 4a of volume 1 of DoD Manual 1000.13, "DoD Identification (ID) Cards: ID Card Life-Cycle" (available at http://www.dtic.mil/whs/directives/corres/pdf/100013_vol1.pdf) by presenting two forms of government-issued ID, one of which must contain a photograph. The requirement for the primary ID to have a photo cannot be waived. Identity documents must be original or a certified copy. All documentation not in English must have a certified English translation.

(B) Proof of address. DS Logon credential applicants must present proof of address, if address on the presented ID is different than the address in DEERS.

(C) DD Form 214, "Certificate of Release or Discharge from Active Duty." DS Logon credential applicants must present a DD Form 214 if a veteran who was separated before 1982. If separated from the Reserve Component, a DS Logon credential applicant may present a Reserve Component separation document in lieu of a DD Form 214.

(2) Use. DS Logon credential holders may use their DS Logon credential at the My Access Center website and any other DoD self-service website that accepts DS Logon.

(3) Maintenance. DS Logon credential holders may use the My Access Center website to maintain and update their DS Logon credential and manage their personal settings. The DS Logon credential holder may:

(i) Activate or deactivate an account.

(ii) Reset password.

(iii) Update challenge questions and answers.

(iv) Upgrade from a Basic DS Logon to a Premium DS Logon credential.

(v) Select or update preferred sponsor, if a dependent of two sponsors.

(vi) Manage personal and advanced security settings.

(vii) Manage contact information.

(viii) Manage relationships and access granting.

(ix) Manage the DS Logon credential using additional capabilities as implemented by the Director, DMDC.

(4) Decomissioning. DS Logon credentials may be decommissioned by the DS Logon credential holder, via self-service; by an operator, at the request of the DS Logon credential holder; or by the system, when the credential holder no longer has an affiliation to the DoD or is identified as deceased in DEERS.

(5) Reactivation. DS Logon credentials may be reactivated if the person is living and still eligible for the credential.

(d) Associations. DS Logon supports several types of associations, including DEERS-identified family relationships and operator-initiated and -approved surrogates.

(1) Family. Individuals are connected to one another based on their family relationship information in DEERS. A family relationship must exist in DEERS before the relationship can exist in DS Logon.

(i) Multiple sponsors. An individual has only one DS Logon credential, regardless of the number of sponsors the individual has (e.g., a dependent child whose parents are both Service members).

(ii) Transferring families. If an individual has a second family in DEERS, the individual can move their DS Logon credential to the second family. This changes the assignment of the DS Logon credential from the first family to the second family and removes any granted permissions from the first family.

(2) Surrogacy. Surrogacy is a feature that allows an individual who may not be affiliated with the DoD and who may not be related to the DS Logon credential holder or eligible individual by a DoD-recognized family relationship to be granted access to a DS Logon credential holder's or an eligible individual's information. A surrogate may be established as the custodian of a deceased Service member's unmarried minor child(ren) who is under 18, who is at least 18 but under 23 and attending school full-time, or who is incapacitated. A surrogate may also be established as the agent of an incapacitated dependent (e.g., spouse, parent) or of a wounded, ill, or incapacitated Service member.

(i) Eligibility. An operator must first establish an identity in DEERS before establishing the surrogacy association in DS Logon. To establish a surrogate association, the surrogate must present to an operator for approval:

(A) A completed and signed DD Form 3005, "Application for Surrogate Association for DoD Self-Service (DS) Logon."

(B) Any additional eligibility documents required by the DD Form 3005 which describe the scope of the surrogate's authority.

(C) Proof of identity, in accordance with the requirements for in-person proofing in paragraph (c)(1)(iii) of this section.

(ii) Types of surrogates—(A) Financial agent (FA). An eligible individual names an FA to assist with specific financial matters.

(B) Legal agent (LA). An eligible individual names an LA to assist with legal matters.

(C) Caregiver (CG). An eligible individual names a CG to assist with general health care requirements (example, viewing general health-care related information, scheduling appointments, refilling prescriptions, and tracking medical expenses), but does not make health care decisions.

(D) Health care agent (HA). An eligible individual (the patient) names an HA in a durable power of attorney for health care documents to make health care decisions.

(E) Legal guardian (LG). An LG is appointed by a court of competent jurisdiction in the United States (or jurisdiction of the United States) to make legal decisions for an eligible individual.

(F) Special guardian (SG). An SG is appointed by a court of competent jurisdiction in the United States (or jurisdiction of the United States) for the specific purpose of making health care-related decisions for an eligible individual.

(e) Permissions. A sponsor, a sponsor's spouse, and a sponsor's dependent over the age of 18 can manage who has access to their information (i.e., who has access to view and edit their information and who is eligible to act on their behalf). The provisions of this section may be superseded by order of a court of competent jurisdiction.

(1) Sponsor access. Sponsors will automatically have access to the information of all dependents under the age of 18.

(2) Spousal access—(i) Automatic. A sponsor's spouse will automatically have access to the information of all dependent children under the age of 18 whose relationship to the sponsor began on or after the date of marriage of the sponsor and sponsor's spouse.

(ii) Sponsor-granted. The sponsor may grant the sponsor's spouse access to the information of dependent children under the age of 18 whose relationship to the sponsor began before the date of marriage of the sponsor and the sponsor's spouse.

(3) Granted access. A sponsor, a sponsor's spouse, and a sponsor's dependent over the age of 18 may grant access to their information via the My Access Center website in accordance with paragraph (c)(3) of this section. Surrogate access to the information of a sponsor, a sponsor's spouse, and a sponsor's dependent (regardless of age) must be granted via in-person proofing, including the submission of eligibility documents to an operator for approval in accordance with paragraph (d)(2) of this section.

(i) Access granting by a sponsor. Sponsors may grant their spouse access to the sponsor's information and the information of any sponsor's dependents under the age of 18. Access to the sponsor's information and the information of any sponsor's dependents under the age of 18 may not be granted to any other sponsor's dependent, unless that dependent has been identified as a surrogate.

(ii) Access granting by a spouse. Spouses may grant the sponsor access to the spouse's information. Access to the spouse's information may not be granted to any other sponsor's dependent, unless that sponsor's dependent has been identified as a surrogate.

(iii) Access granting by a dependent over 18. A sponsor's dependent over the age of 18 may grant the sponsor and the sponsor's spouse access to the dependent's information. Access to the information of a sponsor's dependent over the age of 18 may not be granted to any other sponsor's dependent, unless that sponsor's dependent has been identified as a surrogate.

Dated: October 27, 2016.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2016-26416 Filed: 11/1/2016 8:45 am; Publication Date: 11/2/2016]