Rules and Regulations

Federal Register
Vol. 70, No. 203
Friday, October 21, 2005

OFFICE OF PERSONNEL MANAGEMENT

5 CFR Part 532

RIN 3206–AK83

Prevailing Rate Systems; Redefinition of the Central North Carolina Appropriated Fund Wage Area

AGENCY: Office of Personnel Management.

ACTION: Final rule.

SUMMARY: The Office of Personnel Management is issuing a final rule to redefine the geographic boundaries of the Central North Carolina Federal Wage System (FWS) appropriated fund wage area. The final rule removes Edgecombe and Wilson Counties, NC, from the survey area and adds Hoke County, NC, to the survey area. The redefinition of Edgecombe, Hoke, and Wilson Counties aligns the geographic definition of the Central North Carolina wage area more closely with the regulatory criteria used to define FWS wage areas.

DATES: This rule is effective on November 21, 2005.

FOR FURTHER INFORMATION CONTACT: Madeline Gonzalez, (202) 606–2838; e-mail *pay-performance-policy@opm.gov*; or FAX: (202) 606–4264.

SUPPLEMENTARY INFORMATION: On May 18, 2005, the Office of Personnel Management (OPM) issued a proposed rule (70 FR 28488) to remove Edgecombe and Wilson Counties, NC, from the Central North Carolina survey area and add Hoke County, NC, to the survey area. The proposed rule had a 30-day comment period, during which OPM received no comments.

Regulatory Flexibility Act

I certify that these regulations will not have a significant economic impact on a substantial number of small entities because they will affect only Federal agencies and employees.

List of Subjects in 5 CFR Part 532

Administrative practice and procedure, Freedom of information, Government employees, Reporting and recordkeeping requirements, Wages.

Office of Personnel Management.

Linda M. Springer,

Director.

■ Accordingly, the Office of Personnel Management is amending 5 CFR part 532 as follows:

PART 532—PREVAILING RATE SYSTEMS

■ 1. The authority citation for part 532 continues to read as follows:

Authority: 5 U.S.C. 5343, 5346; § 532.707 also issued under 5 U.S.C. 552.

■ 2. In appendix C to subpart B, the wage area listing for the State of North Carolina is amended by revising the listing for Central North Carolina to read as follows:

Appendix C to Subpart B of Part 532—Appropriated Fund Wage and Survey Areas

* * * * *

North Carolina

Central North Carolina

Survey Area

North Carolina: Cumberland, Durham, Harnett, Hoke, Johnston, Orange, Wake, Wayne.

Area of Application. Survey area plus:

North Carolina: Alamance, Bladen, Caswell, Chatham, Davidson, Davie, Edgecombe, Franklin, Forsyth, Granville, Guilford, Halifax, Lee, Montgomery, Moore, Nash, Northampton, Person, Randolph, Richmond, Robeson, Rockingham, Sampson, Scotland, Stokes, Surry, Vance, Warren, Wilson, and Yadkin.

South Carolina: Dillon, Marion, and Marlboro.

* * * * *

[FR Doc. 05–21050 Filed 10–20–05; 8:45 am]

BILLING CODE 6325–39–U

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 7

RIN 1601–AA02

Classified National Security Information

AGENCY: Office of the Secretary, DHS.

ACTION: Final rule.

SUMMARY: This final rule revises the Department of Homeland Security's procedures for managing classified national security information. This rule implements procedures required under Executive Order 12958, ''Classified National Security Information,'' as amended by Executive Order 13292, and amends the initial procedures established when the Department was created in January 2003. Further, this rule delegates to the Chief Security Officer of the Department of Homeland Security the responsibility of serving as the ''Senior Agency Official'' pursuant to Executive Order 12958, as amended.

DATES: This final rule is effective October 21, 2005.

FOR FURTHER INFORMATION CONTACT: John J. Young, Chief, Administrative Security Division, Office of Security, Department of Homeland Security, (202) 772–9614 (not a toll free call).

SUPPLEMENTARY INFORMATION:

I. Background

On November 25, 2002, the President signed into law the Homeland Security Act of 2002, Public Law 107–296, 116 Stat. 2135 (6 U.S.C. 101 *et seq.*) (HSA), creating the Department of Homeland Security (DHS). DHS is comprised of 22 Federal agencies brought together for the common goals of preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing damage and assisting in recovery from attacks that occur in the United States.

DHS came into existence on January 24, 2003 under section 4 of the HSA, 116 Stat. at 2142 (6 U.S.C. 101 note). In order to facilitate public interaction with DHS's Office of the Secretary and to meet the mandate set forth in Executive Order 12958, as amended, DHS issued an interim final rule to establish an initial set of procedures for

the classification, safeguarding and declassification of classified national security information. 68 FR 4703 (Jan. 27, 2003). Because the procedures implemented under the January 27, 2003 interim final rule were determined by DHS to be agency procedural rules, the interim rule was exempt from prior notice and public comment under the Administrative Procedure Act (APA) (5 U.S.C. 553) and became effective upon publication.

On March 25, 2003, the President issued Executive Order 13292, 68 FR 15315 (March 28, 2003), which further amended Executive Order 12958. Executive Order 12958, as amended, further directed Federal agencies to designate a Senior Agency Official to direct and administer the program for handling classified national security information. Among the responsibilities of the Senior Agency Official is the promulgation of implementing regulations that are required to be published in the **Federal Register** to the extent such regulations affect the public.

DHS is promulgating this final rule, consistent with the mandates set forth under Executive Order 12958, as amended, to establish procedures, and revise existing DHS procedures for the classification, safeguarding and declassification of classified national security information. This final rule is consistent with similar rules of other Executive agencies relating to procedures for the classification, safeguarding and declassification of classified national security information.

II. Analysis of This Final Rule

This final rule establishes the procedures necessary for DHS to fulfill its obligations under Executive Order 12958, as amended, ''Classified National Security Information.'' This final rule is not intended to address or satisfy obligations mandated to the Department under Executive Orders 13311, Homeland Security Information Sharing, 68 FR 45149 (July 31, 2003) or Executive Order 13356, Strengthening the Sharing of Terrorism Information to Protect Americans, 69 FR 53599 (September 1, 2004).

Subpart A—Administration

Subpart A delegates responsibility for administration of the DHS classification management program to the Chief Security Officer who shall act in the capacity of ''Senior Agency Official'' as defined in E.O. 12958, as amended. This delegation had been previously assigned to the Under Secretary for Information Analysis and Infrastructure Protection (IAIP) under the predecessor DHS Interim Final Rule dated January 27, 2003. It also mandates responsibility to the components for designation of a security officer/security liaison to implement and oversee the program at each component. Subpart A sets forth potential sanctions that may be imposed pursuant to E.O. 12958, as amended. These sanctions are independent of criminal penalties under 18 U.S.C. 371, 792–798, 1001; the Act of September 23, 1950, ch. 1024, tit. I, section 4, 64 Stat. 991, as amended (50 U.S.C. 783); and the National Security Act of 1947, ch. 343, tit. VI, section 601, as added by the Intelligence Identities Protection Act of 1982, Public Law 97–200, section 2, 96 Stat. 122 (June 23, 1982), as amended (50 U.S.C. 421), or other laws. Each of these provisions of law may impose sanctions against persons who commit a violation in the handling of classified information and it outlines policy for the introduction of classified information into judicial proceedings.

Subpart B—Classified Information

Subpart B provides DHS policy on the classification and declassification of national security information and provisions for the release of classified information to uncleared persons in an emergency. Subpart B also provides the DHS processes for challenging the classification of information and, as it applies to the public, submitting a request for a mandatory review of classified information for declassification and public release. It also establishes the DHS Classification Appeals Panel (DHS/CAP) for the purpose of reviewing appeals of denial for declassification.

III. Regulatory History

Administrative Procedure Act

DHS is implementing this rule without notice and the opportunity for public comment as this rule involves DHS management and organization, and DHS internal procedures for the classification and handling of classified national security information. Therefore, this rule is exempt from the rulemaking requirements under 5 U.S.C. 553 pursuant to the exclusions in section 553(a). Further, this rule generally parallels the procedures currently used by other agencies to fulfill their obligations under Executive Order 12958, as amended, regarding classified national security information. Implementation of this rule without notice and the opportunity for public comment is warranted also under the ''good cause'' standard found under 5 U.S.C. 553(b) because it implements only national security interests relating to classified information and does not affect the rights of the general public. For the same reasons, the Department has determined that this final rule should be issued without a delayed effective date pursuant to 5 U.S.C. 553(d)(3).

Regulatory Flexibility Act

DHS, in accordance with the Regulatory Flexibility Act, 5 U.S.C. 605(b), has reviewed this final rule and, by approving it, certifies that it will not have a significant economic impact on a substantial number of small entities because it pertains to personnel and administrative matters affecting the Department. Further, a Regulatory Flexibility Analysis is not required for this final rule because the Department was not required to publish a general notice of proposed rulemaking for this matter.

Executive Order 12866

This rule has been drafted and reviewed in accordance with Executive Order 12866, Regulatory Planning and Review, section 1(b), Principles of Regulation. This rule is not a significant regulatory action under section 3(f) of Executive Order 12866.

Executive Order 12988

This regulation meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988, Civil Justice Reform.

Executive Order 13132

This rule will 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. Therefore, in accordance with Executive Order 13132, DHS has determined that this rule does not have sufficient federalism implications to warrant the preparation of a federalism summary impact statement.

Unfunded Mandates Reform Act of 1995

This rule will not result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year, and it will not significantly or uniquely affect small governments. Therefore, no actions are necessary under the provisions of the Unfunded Mandates Reform Act of 1995, 2 U.S.C. 1501 *et seq.*

Small Business Regulatory Enforcement Fairness Act of 1996

This rule is not a major rule as defined by section 251 of the Small

Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), 5 U.S.C. 804. This rule will not result in an annual effect on the economy of $100 million or more, a major increase in costs or prices, or significant adverse effects on competition, employment, investment, productivity, innovation, or the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and export markets.

National Environmental Policy Act of 1969

DHS has reviewed this action for purposes of the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321–4347) and has determined that this action will not have a significant effect on the human environment.

Executive Order 12958, as Amended

This Final Rule has been reviewed by the Information Security Oversight Office of the National Archives and Records Administration, pursuant to Executive Order 12958, as amended.

List of Subjects in 6 CFR Part 7

Classified information, Organization, functions, and authority delegations.

■ Accordingly, for the reasons set forth above, 6 CFR chapter I, part 7, is revised to read as follows:

PART 7—CLASSIFIED NATIONAL SECURITY INFORMATION

Sec.

Authority: 5 U.S.C. 301; Pub. L. 107–296, 116 Stat. 2135 (6 U.S.C. 101); E.O. 12958, 60 FR 19825, 3 CFR, 1995 Comp., p. 333; E.O. 13142, 64 FR 66089, 3 CFR, 1999 Comp., p. 236; 32 CFR part 2001.

§ 7.1 Purpose.

The purpose of this part is to ensure that information within the Department of Homeland Security (DHS) relating to the national security is classified, safeguarded, and declassified pursuant to the provisions of Executive Order 12958, as amended, and implementing directives from the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA).

§ 7.2 Scope.

(a) This part applies to all employees, detailees and non-contractor personnel outside the Executive Branch who are granted access to classified information by the DHS, in accordance with the standards in Executive Order 12958, as amended, and its implementing directives.

(b) This part does not apply to contractors, grantees and other categories of personnel falling under the purview of Executive Order 12829, National Industrial Security Program, and its implementing directives.

(c) This part is independent of and does not affect any classification procedures or requirements of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 *et seq*).

(d) This part does not, and is not intended to, create any right to judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person. This part creates limited rights to administrative review of decisions. This part does not, and is not intended to, create any right to judicial review of administrative action.

§ 7.3 Definitions.

The terms defined or used in Executive Order 12958, as amended, and the implementing directives in 32 CFR parts 2001 and 2004, are applicable to this part.

Subpart A—Administration

§ 7.10 Authority of the Chief Security Officer, Office of Security.

(a) The DHS Chief Security Officer (hereafter ''Chief Security Officer'') is designated as the Senior Agency Official as required by section 5.4(d) of Executive Order 12958, as amended, and, except as specifically provided elsewhere in this part, is authorized to administer the DHS Classified National Security Information program pursuant to Executive Order 12958, as amended.

(b) The Chief Security Officer shall, among other actions:

(1) Oversee and administer the DHS's program established under Executive Order 12958, as amended;

(2) Promulgate implementing regulations;

(3) Establish and maintain Department-wide security education and training programs;

(4) Establish and maintain an ongoing self-inspection program including the periodic review and assessment of the DHS's classified product;

(5) Establish procedures to prevent unnecessary access to classified information, including procedures that:

(i) Require that a need for access to classified information is established before initiating administrative procedures to grant access; and

(ii) Ensure that the number of persons granted access to classified information is limited to the minimum necessary for operational and security requirements and needs;

(6) Develop special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) Coordinate with the DHS Chief Human Capital Officer, as appropriate to ensure that the performance contract or other system used to rate personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of:

(i) Original classification authorities;

(ii) Security managers or security specialists; and

(iii) All other personnel whose duties significantly involve the creation or handling of classified information;

(8) Account for the costs associated with implementing this part and report the cost to the Director of ISOO;

(9) Assign in a prompt manner personnel to respond to any request, appeal, challenge, complaint, or suggestion concerning Executive Order 12958, as amended, that pertains to classified information that originated in a DHS component that no longer exists and for which there is no clear successor in function;

(10) Report violations, take corrective measures and assess appropriate sanctions as warranted, in accordance with Executive Order 12958, as amended;

(11) Overseeing DHS participation in special access programs authorized under Executive Order 12958, as amended;

(12) Direct and administer DHS's personnel security program in

accordance with Executive Order 12968 and other applicable law;

(13) Direct and administer DHS implementation and compliance with the National Industrial Security Program in accordance with Executive Order 12829 and other applicable guidance; and

(14) Perform any other duties as the Secretary may designate.

(c) The Chief Security Officer shall maintain a current list of all officials authorized pursuant to this part to originally classify or declassify documents.

§ 7.11 Components' responsibilities.

Each DHS component shall appoint a security officer or security liaison to implement this part. the security officer/security liaison shall:

(a) Implement, observe, and enforce security regulations or procedures within their component with respect to the classification, declassification, safeguarding, handling, and storage of classified national security information;

(b) Report violations of the provisions of this regulation to the Chief Security Officer committed by employees of their component, as required;

(c) Ensure that employees of their component acquire adequate security education and training, as required by the DHS classified information security procedures;

(d) Continuously review the requirements for personnel access to classified information as a part of the continuous need-to-know evaluation, and initiate action to administratively withdraw or reduce the level of access authorized, as appropriate; and

(e) Cooperate fully with any request from the Chief Security Officer for assistance in the implementation of this part.

§ 7.12 Violations of classified information requirements.

(a) Any person who suspects or has knowledge of a violation of this part, including the known or suspected loss or compromise of classified information, shall promptly report such violations or possible violations, pursuant to requirements set forth in DHS directives.

(b) DHS employees and detailees may be reprimanded, suspended without pay, terminated from classification authority, suspended from or denied access to classified information, or subject to other sanctions in accordance with applicable law and DHS regulations or directives if they:

(1) Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under Executive Order 12958, as amended, or its predecessor orders;

(2) Knowingly, willfully, or negligently classify or continue the classification of information in violation of Executive Order 12958, as amended, or its implementing directives; or

(3) Knowingly, willfully, or negligently violate any other provision of Executive Order 12958, as amended, or DHS implementing directives, or;

(4) Knowingly, willfully, or negligently grant eligibility for, or allow access to, classified information in violation of Executive Order 12958, or its implementing directives, this part, or DHS implementing directives promulgated by the Chief Security Officer.

§ 7.13 Judicial proceedings.

(a) Any DHS official or organization receiving an order or subpoena from a Federal or State court, or an administrative subpoena from a Federal agency, to produce classified information (see 6 CFR 5.41 through 5.49), required to submit classified information for official DHS litigative purposes, or receiving classified information from another organization for production of such in litigation, shall notify the Office of the General Counsel, unless the demand for production is made by the Office of the General Counsel, and immediately determine from the agency originating the classified information whether the information can be declassified. If declassification is not possible, DHS representatives will take appropriate action to protect such information, pursuant to the provisions of this section.

(b) If a determination is made to produce classified information in a judicial proceeding in any manner, the DHS General Counsel attorney, in conjunction with the Department of Justice, shall take appropriate steps to protect classified information in judicial proceedings and retrieve the information when the information is no longer required in such judicial proceedings, in accordance with the Department of Justice procedures, and in Federal criminal cases, pursuant to the requirements of Classified Information Procedures Act (CIPA), Public Law 96–456, 94 Stat. 2025, (18 U.S.C. App.), and the ''Security Procedures Established Pursuant to Public Law 96–456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information,'' and other applicable authorities.

Subpart B—Classified Information

§ 7.20 Classification and declassification authority.

(a) Top Secret original classification authority may only be exercised by the Secretary of Homeland Security and by officials to whom such authority is delegated in writing by the Secretary. The Chief Security Officer, as the Senior Agency Official, is delegated authority to originally classify information up to and including Top Secret. No official who is delegated Top Secret original classification authority by the Secretary may further delegate such authority.

(b) The Chief Security Officer may delegate Secret and Confidential original classification authority to other officials determined to have frequent need to exercise such authority. No official who is delegated original classification authority by the Secretary or the Chief Security Officer may further delegate such authority.

(c) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level. In the absence of an official authorized to exercise classification authority, the person designated to act in lieu of such official may exercise the official's classification authority.

§ 7.21 Classification of information, limitations.

(a) Information may be originally classified only if all of the following standards are met:

(1) An original classification authority is classifying the information;

(2) The information is owned by, produced by or for, or is under the control of the United States Government;

(3) The information falls within one or more of the categories of information specified in section 1.4 of Executive Order 12958, as amended; and

(4) The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and such official is able to identify or describe the damage.

(b) Information shall be classified as Top Secret, Secret, or Confidential in accordance with and in compliance with the standards and criteria in Executive Order 12958, as amended. No other terms shall be used to identify United States classified information except as otherwise provided by statute.

(c) Information shall not be classified in order to:

(1) Conceal inefficiency, violations of law, or administrative error;

(2) Prevent embarrassment to a person, organization, or agency;

(3) Restrain competition;

(4) Prevent or delay release of information that does not require protection in the interest of national security.

(d) Information may be reclassified after it has been declassified and released to the public under proper authority only in accordance with the following conditions:

(1) The reclassification action is taken under the personal authority and with the written approval of the Secretary or Deputy Secretary of Homeland Security, based on the determination that the reclassification of the information is necessary in the interest of the national security;

(2) The reclassification of the information meets the standards and criteria for classification pursuant to Executive Order 12958, as amended;

(3) The information may be reasonably recovered; and

(4) The reclassification action is reported promptly to the Director of ISOO.

(e) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after DHS has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of Executive Order 12958, as amended, section 3.5. When it is necessary to classify or reclassify such information, it shall be forwarded to the Chief Security Officer and classified or reclassified only at the direction of the Secretary or Deputy Secretary of Homeland Security.

§ 7.22 Classification pending review.

(a) Whenever persons who do not have original classification authority originate or develop information that they believe requires immediate classification and safeguarding, and no authorized classifier is available, that person shall:

(1) Safeguard the information in a manner appropriate for the classification level they believe it to be;

(2) Apply the appropriate overall classification markings; and

(3) Within five working days, securely transmit the information to the organization that has appropriate subject matter interest and classification authority.

(b) When it is not clear which component would be the appropriate original classifier, the information shall be sent to the Chief Security Officer to determine the appropriate organization.

(c) The organization with classification authority shall decide within 30 days whether to classify the information.

§ 7.23 Emergency release of classified information.

(a) The Secretary of Homeland Security has delegated to certain DHS employees the authority to disclose classified information to an individual or individuals not otherwise routinely eligible for access in emergency situations when there is an imminent threat to life or in defense of the homeland.

(b) In exercising this authority, the delegees shall adhere to the following conditions:

(1) Limit the amount of classified information disclosed to a minimum to achieve the intended purpose;

(2) Limit the number of individuals who receive it to only those persons with a specific need-to-know;

(3) Transmit the classified information through approved communication channels by the most secure and expeditious method possible, or by other means deemed necessary in exigent circumstances;

(4) Provide instructions about what specific information is classified and how it should be safeguarded. Physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary circumstances as determined by the delegated official;

(5) Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain from the recipients a signed DHS Emergency Release of Classified Information Non-disclosure Form. In emergency situations requiring immediate verbal release of information, the signed nondisclosure agreement memorializing the briefing may be received after the emergency abates;

(6) Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 7 days after the release, the disclosing authority must notify the DHS Chief Security Officer and the originating agency of the information disclosed. A copy of the signed nondisclosure agreements should be forwarded with the notification under this paragraph (b)(6), or as soon thereafter as practical.

(7) Release of information pursuant to this authority does not constitute declassification of the information.

(8) Authority to disclose classified information may not be further delegated.

§ 7.24 Duration of classification.

(a) At the time of original classification, original classification authorities shall apply a date or event in which the information will be automatically declassified.

(b) The original classification authority shall attempt to establish a specific date or event not more than 10 years after the date of origination in which the information will be automatically declassified. If the original classification authority cannot determine an earlier specific date or event it shall be marked for automatic declassification 10 years from the date of origination.

(c) If the original classification authority determines that the sensitivity of the information requires classification beyond 10 years, it may be marked for automatic declassification for up to 25 years from the date of original classification decision.

(d) Original classification authorities do not have the authority to classify or retain the classification of information beyond 25 years from the date of origination. The only exception to this rule is when disclosure of the information could be expected to reveal the identity of a confidential human source or human intelligence source. In this instance, the information may be marked for declassification as ''25X1–Human,'' indicating that the information is exempt from the ''25 Year Rule'' for automatic declassification. This marking is not authorized for use when the information pertains to non-human intelligence sources or intelligence methods. In all other instances, classification beyond 25 years shall only be authorized in accordance with § 7.28 of this part and Executive Order 12958, as amended.

§ 7.25 Identification and markings.

(a) Classified information must be marked pursuant to the standards set forth in section 1.6 of Executive Order 12958, as amended; 32 CFR part 2001, subpart B; and internal DHS guidance provided by the Chief Security Officer.

(b) Foreign government information shall retain its original classification markings or be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(c) Information assigned a level of classification under predecessor Executive Orders shall remain classified at that level of classification, except as otherwise provided herein, *i.e.*, the information is reclassified or declassified.

§ 7.26 Derivative classification.

(a) Derivative classification is defined as the incorporating, paraphrasing,

restating, or generating in a new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Information is also derivatively classified when classification is based on instructions provided in a security classification guide.

(b) Persons need not possess original classification authority to derivatively classify information based on source documents or classification guides.

(c) Persons who apply derivative classification markings shall observe original classification decisions and carry forward to any newly created documents the pertinent classification markings.

(d) Information classified derivatively from other classified information shall be classified and marked in accordance with the standards set forth in sections 2.1 and 2.2 of Executive Order 12958, as amended, 32 CFR 2001.22, and internal DHS guidance provided by the Chief Security Officer.

§ 7.27 Declassification and downgrading.

(a) Classified information shall be declassified as soon as it no longer meets the standards for classification. Declassification and downgrading is governed by Part 3 of Executive Order 12958, as amended, implementing ISOO directives at 32 CFR part 2001, subpart C, and applicable internal DHS direction provided by the Chief Security Officer.

(b) Information shall be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position, the originator's successor, or a supervisory official of either, or by officials delegated such authority in writing by the Secretary of Homeland Security or the Chief Security Officer.

(c) It is presumed that information that continues to meet the classification requirements under Executive Order 12958, as amended, requires continued protection. In some exceptional cases during declassification reviews, the need to protect classified information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. If it appears that the public interest in disclosure of the information may outweigh the need to protect the information, the declassification reviewing official shall refer the information with a recommendation for decision to the Chief Security Officer. The Chief Security Officer shall review the information and make a recommendation to the Secretary on whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. The Secretary shall decide whether to declassify the information. The decision of the Secretary shall be final. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural rights subject to judicial review.

(d) Each component shall develop schedules for declassification of records in the National Archives.

§ 7.28 Automatic declassification.

(a) Subject to paragraph (b) of this section, all classified information contained in records that are more than 25 years old that have been determined to have permanent historical value shall be declassified automatically on December 31, 2006. Subsequently, all classified information in such records shall be automatically declassified not later than 25 years after the date of its original classification with the exception of specific information exempt from automatic declassification pursuant to section 3.3 (b) through (d) of Executive Order 12958, as amended.

(b) At least 180 days before information is declassified automatically under this section, the Chief Security Officer shall notify the ISOO of any specific information that DHS proposes to exempt from automatic declassification. The notification shall include:

(1) A description of the information;

(2) An explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

(3) A specific date or event for declassification of the information whenever the information exempted does not identify a confidential human source or human intelligence source.

(c) Proposed exemptions under this section shall be forwarded to the Chief Security Officer. When the Chief Security Officer determines the exemption request is consistent with this section, he or she will submit the exemption request to the Executive Secretary of the Interagency Security Classification Appeals Panel (ISCAP) for approval.

(d) Declassification guides that narrowly and precisely define exempted information may be used to exempt information from automatic declassification. Declassification guides must include the exemption notification information detailed in paragraph (b) of this section, and be approved pursuant to paragraph (c) of this section.

§ 7.29 Documents of permanent historical value.

The original classification authority, to the greatest extent possible, shall declassify classified information contained in records determined to have permanent historical value under 44 U.S.C. 2107 before they are accessioned into the National Archives.

§ 7.30 Classification challenges.

(a) Authorized holders of information classified by DHS who, in good faith, believe that specific information is improperly or unnecessarily classified are encouraged and expected to challenge the classification status of that information pursuant to section 1.8 of Executive Order 12958, as amended. Authorized holders may submit classification challenges in writing to the original classification authority with jurisdiction over the information in question. If an original classification authority cannot be determined, the challenge shall be submitted to the Chief Security Officer. The challenge need not be more specific than a question as to why the information is or is not classified, or is classified at a certain level.

(b) If anonymity of the challenger is requested, the challenger may submit the challenge to the Office of Security. The Office of Security will act as an agent for the challenger and the identity of the challenger will be redacted.

(c) The original classification authority shall promptly, and in no case later than 60 days, provide a written response to the submitter. The original classification authority may classify or declassify the information subject to the challenge and, if applicable, state specific reasons why the original classification determination was proper. If the original classification authority is not able to respond within 60 days, he or she shall inform the individual who filed the challenge in writing of that fact, and the anticipated determination date.

(d) The individual challenging the classification will be notified of the determination made by the original classification authority and that the individual may appeal this determination to the Chief Security Officer. Upon receipt of such appeals, the Chief Security Officer shall convene a DHS Classification Appeals Panel (DHS/CAP). The DHS/CAP shall, at a minimum, consist of representatives from the Office of Security, the Office of General Counsel, and a representative from the component having jurisdiction

over the information. Additional members may be added as determined by the DHS Chief Security Officer. The DHS/CAP shall be chaired by the Chief Security Officer.

(e) If the requester files an appeal through the DHS/CAP, and the appeal is denied, the requester shall be notified of the right to appeal the denial to the Interagency Security Classification Appeals Panel (ISCAP) pursuant to section 5.3 of Executive Order 12958, as amended, and the rules issued by the ISCAP pursuant to section 5.3 of Executive Order 12958, as amended.

(f) Any individual who challenges a classification and believes that any action has been taken against him or her in retaliation or retribution because of that challenge shall report the facts to the Office of the Inspector General or other appropriate office.

(g) Nothing in this section shall prohibit a person from informally challenging the classified status of information directly to the original classification authority.

(h) Requests for review of classified material for declassification by persons other than authorized holders are governed by 6 CFR 7.31.

§ 7.31 Mandatory review for declassification requests.

(a) Any person may request that classified information be reviewed for declassification pursuant to the mandatory declassification review provisions of section 3.6 of Executive Order 12958, as amended. Such requests shall be sent to the Departmental Disclosure Officer, Privacy Office, 245 Murray Lane, SW., Building 410, Washington, DC 20528.

(b) The request must sufficiently describe the document or material with enough specificity to allow it to be located by the component with a reasonable amount of effort. When the description of the information in the request is deficient, the component shall solicit as much additional identifying information as possible from the requester. If the information or material requested cannot be obtained with a reasonable amount of effort, the component shall provide the requester, through the DHS Disclosure Officer, with written notification of the reasons why no action will be taken and of the requester's right to appeal.

(c) Requests for review of information that has been subjected to a declassification review request within the preceding two years shall not be processed. The DHS Disclosure Officer will notify the requester of such denial.

(d) Requests for information exempted from search or review under sections 701, 702, or 703 of the National Security Act of 1947, as added and amended (50 U.S.C. 431 through 433), or other provisions of law, shall not be processed. The DHS Disclosure Officer will notify the requester of such denial.

(e) If documents or material being reviewed for declassification under this section contain information that has been originally classified by another government agency, the reviewing authority shall notify the DHS Disclosure Officer. Unless the association of that organization with the requested information is itself classified, the DHS Disclosure Officer will then notify the requester of the referral.

(f) A DHS component may refuse to confirm or deny the existence, or non-existence, of requested information when its existence or non-existence, is properly classified.

(g) DHS components shall make a final determination on the request as soon as practicable but within one year from receipt. When information cannot be declassified in its entirety, components shall make reasonable efforts to redact those portions that still meet the standards for classification and release those declassified portions of the requested information that constitute a coherent segment.

(h) DHS components shall notify the DHS Disclosure Officer of the determination made in the processing of a mandatory review request. Such notification shall include the number of pages declassified in full; the number of pages declassified in part; and the number of pages where declassification was denied.

(i) The DHS Disclosure Officer shall maintain a record of all mandatory review actions for reporting in accordance with applicable Federal requirements.

(j) The mandatory declassification review system shall provide for administrative appeal in cases where the review results in the information remaining classified. The requester shall be notified of the results of the review and of the right to appeal the denial of declassification. To address such appeals, the DHS Disclosure Office shall convene a DHS Classification Appeals Panel (DHS/CAP). The DHS/CAP shall, at a minimum, consist of representatives from the Disclosure Office, the Office of Security, the Office of General Counsel, and a representative from the component having jurisdiction over the information. Additional members may be added as determined by the DHS Disclosure Officer. The DHS/CAP shall be chaired by the DHS Disclosure Officer.

(k) If the requester files an appeal through the DHS/CAP, and the appeal is denied, the requester shall be notified of the right to appeal the denial to the ISCAP pursuant to section 5.3 of Executive Order 12958, as amended, and the rules issued by the ISCAP pursuant to section 5.3 of Executive Order 12958, as amended.

Dated: October 8, 2005.

Michael Chertoff,

Secretary.

[FR Doc. 05–21011 Filed 10–20–05; 8:45 am]

BILLING CODE 4410–10–U

DEPARTMENT OF AGRICULTURE

Agricultural Marketing Service

7 CFR Part 205

[Docket Number TM–05–02]

National Organic Program (NOP); Amendment to the National List of Allowed and Prohibited Substances (Livestock)

AGENCY: Agricultural Marketing Service, USDA.

ACTION: Final rule.

SUMMARY: This final rule amends the U.S. Department of Agriculture's (USDA) National List of Allowed and Prohibited Substances (National List) to reflect one recommendation submitted to the Secretary by the National Organic Standards Board (NOSB) on March 3, 2005. Consistent with the recommendation from the NOSB, this final rule revises the annotation of one substance on the National List, methionine, to extend its use in organic poultry production until October 21, 2008.

EFFECTIVE DATE: This rule becomes effective October 22, 2005.

FOR FURTHER INFORMATION CONTACT: Arthur Neal, Director of Program Administration, Telephone: (202) 720–3252; Fax: (202) 205–7808.

SUPPLEMENTARY INFORMATION:

I. Background

On December 21, 2000, the Secretary established, within the NOP regulations [7 CFR part 205], the National List (§§ 205.600 through 205.607). The National List identifies synthetic substances that are allowed and nonsynthetic substances that are prohibited in organic crop and livestock production. The National List also identifies nonsynthetic and synthetic substances that are allowed for use in certified handling operations. Under the