United States Department of Agriculture
Office of Inspector General

U.S. Department of Agriculture's Office of Homeland Security and Emergency Coordination - Classification Management

Audit Report 61701-0001-32
September 2013

U.S. Department of Agriculture's Office of Homeland Security and Emergency Coordination - Classification Management

Audit Report 61701-0001-32

What Were OIG's Objectives

To assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within USDA; and identify whether they may be contributing to persistent misclassification of material. This audit was required by Public Law 111-258, Reducing Over-Classification Act.

What OIG Reviewed

Our audit examined USDA guidance and 31 documents classified by USDA at the "Secret" and "Top-Secret" level.

What OIG Recommends

USDA should ensure records management, Departmental regulations, procedures, and the classification guide reflect Federal classification requirements, and review all USDA classified documents to correct improper markings. The original classification authority should direct all subordinate agencies to report self-inspections and program statistics. PDSD should develop, record, and track all training that meets Federal requirements.

OIG reviewed USDA's process for classified documents in order to determine if PDSD is adequately managing USDA's classified national security information program, as required by the Reducing Over-Classification Act.

What OIG Found

This is the first of two reports required by the Reducing Over-Classification Act to determine the Department of Agriculture's (USDA) compliance with Federal regulations. The Act was designed to prevent information from being over-classified and over-compartmentalized, and to promote information sharing, as prescribed by Federal guidelines.

The Personnel and Document Security Division (PDSD) focuses on safeguarding national security information within USDA. We found that PDSD lacks proper guidance for eight key areas relating to classification management, and does not have a records management system that would identify documents that need to be declassified or reviewed for continued national security. We also found that USDA's classification guide was missing required elements needed for proper derivative classification decisions. PDSD also needs to improve its reviews of classified markings on documents. Additionally, PDSD does not always obtain and maintain adequate statistics related to the security classification program and USDA does not ensure that its subordinate agencies are conducting self-inspections in accordance with regulations and procedures. Finally, PDSD's classification management training content and documentation need to be improved, particularly in providing required information to individuals with security clearances. As a result, there is a greater potential for over-classifying or improperly releasing national security information.

OIG accepted management decision on 8 of the 17 recommendations; however, further action from the agency is needed before management decision can be reached for the other recommendations.

United States Department of Agriculture

Office of Inspector General

Washington, D.C. 20250

DATE: September 27, 2013

AUDIT NUMBER: 61701-0001-32

TO: Todd Repass, Jr.
Director
Office of Homeland Security and Emergency Coordination

ATTN: Jennifer Wendel
Office of Homeland Security and Emergency Coordination
Audit Liaison

FROM: Gil H. Harden
Assistant Inspector General for Audit

SUBJECT: Classification Management

This report presents the results of the subject audit. Your written response to the official draft report, dated September 19, 2013, is included in its entirety at the end of the report. Excerpts from your response and the Office of Inspector General (OIG) position are incorporated in the relevant Findings and Recommendations sections of the report. Based on the written response, we accept management decision on Recommendations 5, 7, 8, 9, 10, 13, 14, and 15 in the report. However, management decision has not been reached for Recommendations 1, 2, 3, 4, 6, 11, 12, 16, and 17. Management decisions for the recommendations can be reached once you have provided the additional information outlined in the report sections' OIG Position.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned, and timeframes for implementing the recommendations for which management decisions have not been reached. Please note that the regulation requires management decision to be reached on all recommendations within 6 months from report issuance, and final action to be taken within 1 year of each management decision to prevent being listed in the Department's annual Agency Financial Report. Please follow your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audit fieldwork and subsequent discussions.

This report contains publically available information and will be posted in its entirety to our website (http://www.usda.gov/oig) in the near future.

Table of Contents

Background and Objectives 1
Section 1: Classified Management 5
Finding 1: Effectiveness of Security Program Management 5
Recommendation 1 to the Personnel and Document Security Division (PDSD) 10
Recommendation 2 to PDSD 11
Recommendations 3 to the Senior Agency Official (SAO) 11
Finding 2: Effectiveness of Original Classification Authorities 12
Recommendation 4 to the Original Classification Authorities (OCA) 14
Recommendation 5 to PDSD 14
Finding 3: Effectiveness of Original Classification Decisions and Dissemination Control Marking Decisions 15
Recommendation 6 to the OCA 16
Recommendation 7 to PDSD 16
Finding 4: Effectiveness of Derivative Classification Decisions and Dissemination Control Marking Decisions 17
Recommendation 8 to PDSD 19
Recommendation 9 to PDSD 19
Finding 5: Effectiveness of Security Self-Inspection Program 20
Recommendation 10 to the SAO 22
Recommendation 11 to the SAO 22
Recommendation 12 to the OCA 23
Finding 6: Effectiveness of Security Reporting 24
Recommendation 13 to the SAO 25
Recommendation 14 to PDSD 26
Finding 7: Effectiveness of Security Education and Training 27
Recommendation 15 to PDSD 29
Recommendation 16 to PDSD 29
Recommendation 17 to PDSD 30
Scope and Methodology 31
Abbreviations 33

Exhibit A: Effectiveness of Classification Management Policies and Control Marking Guidelines 34
Agency's Response 39

Background and Objectives

Background

Public Law 111-258, *Reducing Over-Classification Act*, section 6(b), requires the Office of Inspector General (OIG) of each Department or agency with an officer or employee who is authorized to make original classifications, in consultation with the Information Security Oversight Office (ISOO),[1] to carry out at least two evaluations before September 30, 2016. The initial evaluation shall be completed by September 30, 2013. The second required evaluation should review progress since the first review and be completed no later than September 30, 2016.

Executive orders since 1940 have directed Governmentwide classification standards and procedures. On December 29, 2009, President Obama signed Executive Order (E.O.) 13526, *Classified National Security Information*, which establishes the current principles, policies, and procedures for classification. The E.O. prescribes a uniform system for classifying, safeguarding, and declassifying national security information. E.O. 13526 also states that this nation's progress depends on the sharing of information, both within the Government and with the American people. Accordingly, protecting information critical to national security and demonstrating a commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

Pursuant to this order, classified information that is determined to require protection against unauthorized disclosure to prevent damage to national security must be marked appropriately to indicate its classified status. The three U.S. classification levels, and correlating expected damage to U.S. security if the information is disclosed inappropriately, are:

- Top Secret – shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security, which the original classification authority is able to identify or describe.
- Secret – shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security, which the original classification authority is able to identify or describe.
- Confidential – shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security, which the original classification authority is able to identify or describe.

Except as otherwise provided by statute, no other terms shall be used to identify U.S. classified information. If significant doubt exists about the appropriate level of classification, information shall be classified at the lower level.

[1] ISOO is responsible to the President for policy and oversight of the Governmentwide security classification system and the National Industrial Security Program. ISOO is a component of the National Archives and Records Administration and receives policy and program guidance from the National Security Council.

Information may be originally classified only by original classification authorities (OCA). These are individuals authorized in writing, either by the President, the Vice President, or agency heads or other officials designated by the President, to initially classify information.

On December 29, 2009, the President designated the Secretary of Agriculture to classify information originally as "Secret." OCAs must receive training on proper classification prior to originally classifying information and at least once per calendar year after that. To make an original classification decision, an OCA must determine if the information meets the following standards for classification:

- The information is owned, controlled, or produced by or for the U.S. Government;
- The information falls within one or more of the eight categories (reasons for classification) of information described in section 1.4 of E.O. 13526; and
- The unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which the OCA is able to identify or describe.

By definition, original classification precedes all other aspects of the security classification system, including derivative classification,[2] safeguarding, and declassification. The term "over-classification" is not defined in national policy. E.O. 13526 does define "classification" and "declassification." During the course of our fieldwork and in this report, we have used a working definition of "over-classification," which was supplied by ISOO: the designation of information as classified, when the information does not meet one or more of the standards for classification under section 1.1 of E.O. 13526. If significant doubt exists about the need to classify information, it should not be classified.

The Office of Homeland Security and Emergency Coordination (OHSEC), formed in 2010, is one of 13 offices that fall under Departmental Management within the U.S. Department of Agriculture (USDA). OHSEC provides Departmental leadership to USDA on Governmentwide initiatives in various areas, including the safeguarding of classified national security information within USDA and managing security clearances. Within OHSEC there are six divisions, including the Personnel and Document Security Division (PDSD).

PDSD focuses on safeguarding national security information within USDA. To accomplish this, PDSD's Information Security Branch is responsible for establishing and implementing USDA's information security program. The Information Security Branch manages the document security classification function, promulgates policies and regulations concerning the safeguarding of national security information, provides technical support on information security matters to USDA agencies and staff offices, and conducts information security training.

The *USDA Classified National Security Information Program Regulation* (Departmental Regulation (DR) 3440-001) was issued on October 5, 2011, to prescribe Departmental roles and responsibilities for the classification, declassification, and safeguarding of classified national

[2] Derivative classification means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.

security information. This regulation designates the Director of OHSEC as the Senior Agency Official (SAO), or primary liaison between USDA and ISOO, responsible for identifying necessary resources to manage the program and providing program oversight.

Similarly, the *USDA Classified National Security Program Manual* (Departmental Manual (DM) 3440-001), issued on May 1, 2008, establishes the policies and procedures that govern the USDA information security program, which includes uniform requirements and guidance for classifying, safeguarding, declassifying, and destroying classified national security information, whether originated by or released to USDA.

All personnel with an active security clearance can perform derivative classification. All personnel who apply derivative classification markings must receive training on the proper application principles of E.O. 13526 prior to derivatively classifying information and at least once every 2 years thereafter. Information may be derivatively classified from a source document or documents, or through the use of a classification guide.

Federal Government organizations that create or hold classified information are responsible for its proper management. Classification management includes developing classification guides that provide a set of instructions from an OCA to derivative classifiers that identify elements of information regarding a specific subject that must be classified, and the level and duration of classification for each element. One of the most effective ways to protect classified information is through applying standard classification markings and dissemination control markings. Effective program management also includes comprehensive mandatory training for classifiers and a robust self-inspection program.

One of the significant changes to the classification program, pursuant to the issuance of E.O. 13526, is that classified information shall be made accessible to the maximum extent possible to authorized holders. An additional significant change was that classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the recipients meet the criteria for authorized holders, unless the originating agency has obtained approval by ISOO or the Director of National Intelligence, as applicable, to restrict dissemination.

In June 2006,[3] the Government Accountability Office conducted an evaluation of one agency's information security program and found that a lack of oversight and inconsistent implementation of the agency's information security program are increasing the risk of misclassification. Misclassification of national security information impedes effective information sharing, can provide adversaries with information to harm the U.S. and its allies, and incurs millions of dollars in avoidable administrative costs. The Government Accountability Office identified weaknesses in the areas of classification management training, self-inspections, and security classification guide management.

[3] *Managing Sensitive Information: DOD Can More Effectively Reduce the Risk of Classification Errors*, GAO-06-706, June 2006.

Objectives

Public Law 111-258, section 6(b), requires the Office of Inspector General (OIG) of each Department or agency with an officer or employee who is authorized to make original classifications, in consultation with ISOO to:

assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered; and

- identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification.

Section 1: Classified Management

Finding 1: Effectiveness of Security Program Management

USDA needs improvement in its management of the classified national security information program. PDSD does not have a system of records management that facilitates the declassification of documents, pursuant to the provisions of automatic declassification, nor has it updated the Departmental manual (DM 3440-001) to reflect the new requirements of E.O. 13526. This occurred because PDSD considered a records management system to be the same as an inventory of classified information, which is not required. PDSD also has not prioritized updating the Departmental manual. Without a records management system and current policies, there is a potential that USDA documents could be over-classified, documents may be maintained beyond the declassification date (preventing information sharing), and national security information could be released.

General Program Management

General program management refers to the responsibilities of Departments and agencies implementing the program under E.O. 13526.[4] These include the responsibilities of the agency head to demonstrate personal commitment to the program, commit necessary resources to ensure its effective implementation, and to appoint a Senior Agency Official (SAO) to direct and administer the program. The SAO is responsible for overseeing the program established under E.O. 13526, issuing implementing regulations, establishing and maintaining security education and training programs, and establishing and maintaining an ongoing self-inspection program.

We reviewed the classification management program and the use of dissemination control markings to ensure that necessary resources have been dedicated for the effective implementation of the program, that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information, and that an SAO has been designated to direct and administer the program.

According to DR 3080-001, a records management system shall enable the identification, preservation, and retirement of permanent records.[5] Additionally, E.O. 13526 states "to the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification."[6] However, we identified that 8 of the 31 documents we reviewed were being maintained after the declassification date, without having been reviewed for an extension or exemptions, as outlined in the *Mandatory Review for Declassification*.[7] Therefore, the information was not being reviewed to determine if it could be declassified and shared, which in turn has the potential to hinder information sharing.

---

[4] E.O. 13526, December 29, 2009, was published in the *Federal Register* (FR) volume 75, number 2, page 707, January 5, 2010.
[5] *Records Management* (DR 3080-001), April 11, 2007.
[6] 75 FR 707, section 3.2(e), January 5, 2010.
[7] Title 32, *Code of Federal Regulations* (CFR), part 2001.33, July 1, 2010 Edition.

PDSD stated that it did not maintain an inventory of classified documents below the top-secret level because it was not required. While we acknowledge that a complete inventory may not be required, a records management system is required.

Even though an SAO has been assigned to administer the classified national information program, PDSD also needs to dedicate the resources to develop and administer a records management system. Doing so would enable PDSD to identify those documents that need to be reviewed for continued national security or declassified, and reduce the risk of over-classification or a lack of sharing of information.

On August 13, 2013, PDSD staff provided documentation showing that a review of one of the USDA agencies' documents being maintained has been initiated.

Effectiveness of Classification Management Policies and Control Marking Guidelines

Agencies are required to promulgate regulations to implement their classified national security information programs in accordance with E.O. 13526 and 32 *Code of Federal Regulations* (CFR) 2001. We reviewed Departmental Regulation (DR) 3440-001 and Departmental Manual (DM) 3440-001 to determine whether the eight key areas—original classification authority, general program management responsibilities, original classification, derivative classification, declassification, self-inspections, reporting and definitions, and security education and training—were covered and adopted in accordance with the E.O. and the CFR.[8]

Based on our review, we noted that policies had not been adopted in accordance with E.O. 13526 and 32 CFR 2001 for all eight key areas. (See exhibit A for areas where policies need to be addressed.) In addition to the two key areas noted[9] (general program management and classification challenges), we found issues with the remaining six key areas:

- Classification authority: The E.O. provides that the Secretary of Agriculture is designated as the authority to originally classify information to the Secret level and specifically prohibits the Secretary of Agriculture from delegating the authority granted in the order.[10] However, both the Departmental regulation and manual allow the Secretary of Agriculture to re-delegate the authority to the "Deputy Secretary."[11]

- Original classification: The E.O. states "whenever practicable, use a classified addendum." Rather than classifying the entire document, classified addenda would allow

[8] We used *A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258*, Appendix A - *Agency Implementing Regulation Assessment Tool*, which was provided by the Council of the Inspectors General on Integrity and Efficiency to conduct this review. Appendix A focused on eight key areas to determine if applicable classification policies, procedures, rules, and regulations have been adopted in accordance with E.O. 13526 and 32 CFR 2001.

[9] General Program Management and Classification Challenges (Declassification) are covered in separate sections of this finding.

[10] 75 FR 735-736, January 5, 2010.

[11] DR 3440-001 section 5.a., October 5, 2011, and DM 3440-001, chapter 2.1, May 1, 2008.

for "dissemination at the lowest level of classification possible or unclassified form."[12] However, neither the Departmental regulation nor the manual addresses the use of a classified addendum, thereby potentially limiting the information sharing of non-national secure information.

- Derivative classification: According to the E.O. and the CFR, agencies must identify the person applying the derivative classification markings by name and position, or by personal identifier.[13] Because the Departmental manual was last updated in May 2008, approximately 2 years prior to the E.O., it does not address the requirements of identifying the derivative classifier by name and position, nor does it refer to the appropriate criteria.

- Self-inspections: The E.O. and CFR require essential elements of coverage and external reporting of self-inspections.[14] Neither the Departmental regulation nor the manual addresses coverage and external reporting when conducting self-inspections.

- Reporting and definitions: Agencies are required to report to the Director of ISOO any classified information that has been declassified without prior authority, as well as information security violations that: are reported to the Legislative branch; may attract public attention; involve large amounts of information; or reveal a systemic weakness in classification or safeguarding of classified information.[15,16] However, USDA does not have a policy that requires PDSD to report all classified information that has been declassified without prior authority or information security violations.

- Security education and training: The E.O. requires that original and derivative classification authority be "suspended by the agency head or the senior agency official designated" until training has been taken.[17] Neither the Departmental regulation nor the manual provides for suspension of either the original or derivative classification authority (See Finding 7).

In general, PDSD staff agree that the Departmental regulation and manual need to be updated. When we asked why policies had not been updated, staff explained that they were working on a Departmental manual, which they hoped to complete by the end of fiscal year (FY) 2013. They added that it may take time for the Departmental manual to receive final approval, as the last Departmental regulation, which had minimal changes, took more than a year to update.[18] While

[12] 75 FR 707, section 1.6(g), January 5, 2010.
[13] 75 FR 707, section 2.1(b)(1), January 5, 2010, and 32 CFR 2001.22(b), July 1, 2010 Edition.
[14] 75 FR 707, section 5.4(d)(4), January 5, 2010, and 32 CFR 2001.60(e) and (f), July 1, 2010 Edition.
[15] A violation is defined as "any knowing, willful, or negligent action (1) that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or (3) to create or continue a special access program contrary to the requirements of this order."
[16] 75 FR 707, section 5.5(e), January 5, 2010, and 32 CFR 2001.91(a) and (d), July 1, 2010 Edition.
[17] 75 FR 707, section 1.3(d) and 2.1(d), January 5, 2010, and 32 CFR 2001.71(c)(3) and (d)(3), July 1, 2010 Edition.
[18] The changes to the last Departmental regulation primarily added training for the OCA and derivative classifiers, and updated references to E.O. 13526 and the implementing regulation (32 CFR 2001) in various places in the document.

this revision is more substantial, and likely would take more time, PDSD only has two individuals in the Information Security Branch to rewrite the manual, in addition to their other normal duties. Because this revision is an ambitious undertaking, OIG recommends that PDSD dedicate the necessary resources to meet its targeted deadline. Subsequently, staff indicated that USDA is making every effort possible to prioritize available resources in a manner that reflects the Department's needs and the protection of classified information.

Performance Evaluations

According to E.O 13526, properly designating and managing classified information must be a critical element of performance evaluations of personnel whose duties significantly involve handling classified information (such as OCAs and security professionals).

We found that the Departmental regulation (DR 3440-001) did not include the specific language regarding critical elements on performance evaluations needed to comply with E.O. 13526. Specifically, while Departmental regulation requires that performance standards include language that requires all employees who routinely handle classified information to properly protect classified information, the regulation does not require such activity as a critical element or item on the performance evaluation.[19]

However, when we reviewed the *Employee Performance Plan and Appraisal Records* of employees whose duties involved significant handling of classified information, we found that they did contain a critical element on classified material handling that met the requirements of the E.O. Even though this was included on the evaluations, the regulation (DR 3440-001) should be updated to address the requirement of a critical element.

Classification Challenges (Declassification)

E.O. 13526 states that authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information. An agency head or SAO shall establish procedures allowing them to do so. These procedures shall ensure that: individuals are not subject to retribution for bringing such actions; an opportunity is provided for review by an impartial official or panel; and individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (ISCAP).[20]

Additionally, Federal regulations require that if the agency does not respond within 120 days, the challenger has the right to forward the challenge to ISCAP. The challenger may also forward the challenge to the panel if the agency has not responded to an internal appeal within 90 days of the agency's receipt of the appeal. Agency responses to those challenges it denies shall include the challenger's appeal rights to the panel.[21]

[19] DR 3440-001, section 5c(6), October 5, 2011.
[20] 75 FR 707, section 1.8(b), January 5, 2010.
[21] 32 CFR 2001.14(b)(3), July 1, 2010 Edition.

We determined the Departmental regulation and manual do not adequately advise individuals of their rights to appeal to ISCAP or establish procedures to properly process requests to ISCAP for exemptions to automatic declassification. The regulation and manual also do not include the timeframes for challenges to be forwarded to ISCAP. PDSD officials did not agree with this conclusion because the Departmental manual requires classification challenges to be resolved to the extent possible within 30 calendar days of receipt of a challenge. However, we believe that the Departmental manual should be updated so that classifiers are aware of the appeals process and timeframe requirements for sending matters to ISCAP. Without a complete policy in place to establish these processes and the individual's right to appeal, individuals will not have written guidance to challenge the classification status of the information and may not know about their right to appeal to ISCAP (See Finding 7 for training deficiency regarding classification challenges).

Incentives for Accurate Classification

In making cash awards under chapter 45 of title 5, United States Code, the President or head of an executive agency with an officer or employee who is authorized to make original or derivative classification decisions, may consider such officer's or employee's consistent and proper classification of information.[22]

USDA does not offer incentives for accurate classification of information. USDA's OCA responded that "when dealing with classified information 'incentives' are not used to encourage classification or declassification." The classification of information by the OCA "requires an in-depth review," and "[c]lassification management is addressed through user training and awareness."

Sanctions

E.O. 13526 provides that officers and employees of the U.S. Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently: disclose to unauthorized persons information properly classified under this order or predecessor orders; classify or continue the classification of information in violation of this order or any implementing directive; create or continue a special access program contrary to the requirements of this order; or contravene any other provision of this order or its implementing directives.

Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation. If the Director of ISOO finds that a violation has occurred, the Director shall make a report to the head of the agency or to the SAO so that corrective steps, if appropriate, may be taken.

We found that USDA's Departmental manual properly addresses the requirement of sanctions for security infractions and violations. The manual describes an infraction and the action to be

[22] Public Law 111-258, section 6, October 7, 2010.

taken by the supervisor. A security violation is described as a more serious disregard for security procedures and responsibilities. Therefore, disciplinary action will be considered for security violations following the principle of progressive discipline. These actions could be: a reprimand or warning; a suspension without pay; or loss of security clearance or employment.[23]

Conclusions

We found that the agency had not developed a records management system to identify those documents that need to be reviewed for continued national security or declassification. In addition, all eight key areas reviewed were lacking proper guidance in the Departmental regulation and the manual provided to the subordinate agencies and offices. USDA should institute a records management system and update polices to prevent the risk of over-classifying documents, and the potential of improperly releasing national security information.

Recommendation 1 to the Personnel and Document Security Division (PDSD)

Establish a records management system to facilitate the release of information after the declassification date.

Agency Response

In a response dated September 19, 2013, OHSEC officials stated that to ensure classified records are maintained, OHSEC uses DR 3080-001 and E.O. 13526. The ISC [Information Security Coordinator] will be made aware of their responsibility in maintaining a separate classified records management system to the extent possible. Training will be incorporated into the annual refresher and specific training for the ISC will enable the identification, preservation, and retirement of permanent records. The general awareness will be incorporated into the FY 2014 annual refresher training. ISC-specific training will be developed and implemented in AgLearn for all ISCs by the second quarter of 2014.

OIG Position

We are unable to accept management decision at this time. OHSEC's response does not state that a records management system will be developed, only that the ISCs will be made aware of their responsibility along with providing specific training to them.

In order to reach management decision, the response needs to address specific corrective actions that are planned or completed by PDSD to ensure a records management system is developed that will facilitate the release of information after a declassification date and provide an estimated date.

[23] DM 3440-001, chapter 9.5, May 1, 2008.

Recommendation 2 to PDSD

Review all documents in which the declassification date has passed, in accordance with the "Mandatory Review for Declassification."

Agency Response

OHSEC will incorporate specific guidance into the ISC-specific training that addresses the need to review all classified holdings for appropriate markings and control information by the end of the second quarter of FY 2014. This training will include the proper marking elements to ensure all responsible understand the marking and control requirements.

OIG Position

We are unable to accept management decision at this time. The response does not state that documents in which the declassification date has passed will be reviewed. It only addresses that training will be updated to address the need to review all classified holdings.

In order to reach management decision, the response needs to state actions planned or completed by PDSD to ensure that all documents are reviewed in which the mandatory declassification date has passed and an estimated completion date that all documents will be reviewed.

Recommendations 3 to the Senior Agency Official (SAO)

Dedicate the resources to expedite the process of ensuring the Departmental regulation and manual, DR 3440-001 and DM 3440-001, are updated to reflect Federal requirements (E.O. 13526 and 32 CFR 2001).

Agency Response

OHSEC has identified the update of the DM 3440-001 as a critical priority for FY 2014.

OIG Position

We are unable to accept management decision at this time. The response did not provide a date that the Departmental regulation and manual updates will be completed.

In order to reach management decision, an estimated completion date for issuing the updated Departmental regulation and manual needs to be provided.

Finding 2: Effectiveness of Original Classification Authorities

Original Classification Authorities (OCA) are delegated in writing, according to position, by the President, the Vice President, or an agency head or other official designated by the President, to initially classify information. The OCA is responsible for approving, in writing, any classification guide prepared for use by derivative classifiers.

We found that the classification guide developed by USDA[24] was missing required elements needed for proper derivative classification decisions. OIG concluded that this was caused by Departmental omission and officials' misinterpretation of the regulations (See Findings 1 and 7). As a result, derivative classifiers do not have adequate information to make a proper and uniform derivative classification decision, which could lead to a misclassification or over-classification of information.

Designation of Original Classification Authority

We determined that the Secretary of Agriculture was designated to classify information originally as "Secret," by the President, on December 29, 2009, by E.O. which also specified that this authority may not be delegated (See Finding 1 concerning delegation of OCA). [25, 26]

Original Classification Authority Training

As an OCA, the Secretary is authorized to originally classify information, as well as develop classification guides to facilitate the proper and uniform derivative classification of information. To ensure that OCAs are aware of their responsibilities and are equipped to adequately manage the agencies' handling of classified information, they are required to complete training. According to the OCA, initial training was completed in January 2009 and a refresher training in March 2013. However, we found that PDSD did not have documentation confirming that the OCA had completed the required annual training (See Finding 7 regarding OCA training).

USDA Classification Guide

As an OCA, the Secretary of Agriculture is responsible for any classification guide, which, according to regulation, must be prepared to facilitate the proper and uniform derivative classification of information.[27]

At a minimum, classification guides must:

- identify the subject matter of the classification guide;
- identify the original classification authority by name and position, or personal identifier;
- identify an agency point-of-contact for questions regarding the classification guide;

[24] *USDA Carver + Shock Classification Guidance*, July 2010.
[25] 75 FR 735-736, January 5, 2010.
[26] As noted in Finding 1, the Departmental regulation and manual allow the OCA to re-delegate the authority to the "Deputy Secretary."
[27] 32 CFR 2001.15(a), July 1, 2010 Edition.

- provide the date of issuance or last review;
- state precisely the elements of information to be protected;
- state which classification level applies to each element of information;
- state, when applicable, special handling caveats;
- state a concise reason for classification which, at a minimum, cites the classification category in section 1.4 of E.O. 13526; and
- prescribe a specific date or event for declassification.[28]

We found issues with the Department's classification guide that was used by derivative classifiers, and signed by the Secretary of Agriculture on July 19, 2010. Specifically, we found that the classification guide does not:

- identify any agency points-of-contact, or
- prescribe a specific date or event for declassification.

While PDSD staff stated that the classification guide's memorandum identifies various individuals, such as the Assistant Secretary for Administration and the Director, Office of Homeland Security and Emergency Coordination, OIG noted that the memorandum does not specifically identify either of these individuals as a point-of-contact for questions. PDSD staff agreed to update the guide to include a specifically designated point-of-contact.

Lastly, the classification guide gave a range of years (5 to 25), instead of a specific date or event for declassification. PDSD staff stated that the subject matter experts set the duration of classification based on their knowledge because they are the experts. However, the Federal regulation states that information classified derivatively on the basis of a classification guide shall carry forward the markings taken from the instructions in the appropriate classification guide.[29] Thus, OIG concluded that the duration is to be set in the classification guide, by the OCA. PDSD staff did not agree and stated that the subject matter experts are the only ones that can make this decision, but subsequently agreed to work with other Departmental officials to set a specific declassification date by description in the classification guide.

Conclusions

In addition to identifying issues concerning USDA's provisions for OCA delegation and documentation of OCA training (which are detailed in Findings 1 and 7, respectively), we determined that the OCA needs to ensure that the classification guide is updated and compliant with regulations to ensure that it provides derivative classifiers with necessary points-of-contact, as well as a specified date or event for declassification. Because a point-of-contact is not identified on the classification guide, a derivative classifier may not contact the appropriate individual when seeking to obtain information concerning classification of a document, which could result in an incorrect classification decision. Also, because the Department used a range of years, instead of a specific date or event for declassification, the derivative classifier is given the responsibility to make an OCA decision concerning the duration of classification. Both of these

[28] 32 CFR 2001.15(b), July 1, 2010 Edition.
[29] 32 CFR 2001.22(a), July 1, 2010 Edition.

items could lead to a misclassification, over-classification, or unauthorized release of classified national security information.

Recommendation 4 to the Original Classification Authorities (OCA)

Update the classification guide to include a point-of-contact and specific date or event for declassification.

Agency Response

OHSEC believes that further guidance from ISOO is required. OHSEC will provide ISOO's guidance to OIG during the first quarter of FY 2014.

OIG Position

We are unable to accept management decision at this time. The response states that ISOO will be contacted for guidance but does not state that the classification guide will be updated.

In order to reach management decision, the response needs to specify an estimated completion date that the OCA will issue the updated classification guide that includes the required information.

Recommendation 5 to PDSD

Develop and implement procedures to review and update the classification guide when regulatory changes occur to ensure future compliance.

Agency Response

OHSEC will prepare a policy memorandum outlining the new procedures. The memorandum will be distributed by the end of the first quarter of FY 2014.

OIG Position

We accept management decision for this recommendation.

Finding 3: Effectiveness of Original Classification Decisions and Dissemination Control Marking Decisions

Original classification decisions and the proper marking of classified information, to include proper application of dissemination and control markings, need improvement, as USDA did not properly mark classified documents. Specifically, OIG reviewed the two documents that received original classification, during the timeframe covered by our audit, and found that neither had been properly marked to include the OCA's identification or the reason for classification.[30] This occurred because the documents were initially determined to be derivative classifications, but were subsequently changed to original classifications and did not receive updated markings. Individuals relying on these documents as reference material to make derivative classification decisions may not have the necessary information to correctly mark the classified documents, which could result in an over-classification, misclassification, or unauthorized release of classified information.

E.O. 13526, section 1.6, and 32 CFR 2001, subpart C, require that, at the time of classification, originally classified documents shall include the following markings in a manner that is immediately apparent:

- the name and position of the classifier, or personal identifier ("classified by" line);
- agency and office of origin;
- reason for classification;
- declassification instructions ("declassify on" line);
- overall marking;
- portion marking; and
- date of origin of document.

The Food Safety and Inspection Service, a USDA agency, initially marked the two documents as derivative classifications. Specifically, the two documents had the following derivative classification markings: portion markings, overall classification, "declassify on," and "derived from."[31] However, after consultation with PDSD, it was determined that the documents were original classifications, as they contained new information. The OCA classified both documents at the "Secret" level on November 3, 2010, by signing a memorandum.

OIG reviewed these two documents and found that, although the documents were approved as original classifications, the markings on the documents were not updated once the original classification was approved. As a result, the documents do not indicate the reviewer(s) of the documents. A PDSD official confirmed that the markings were not updated. Because of the infrequency of original classification decisions in the Department, a checklist outlining the required markings for the OCA to apply would assist in ensuring documents are appropriately marked.

[30] These two documents were the only original classification documents in USDA in our universe.
[31] For more information on required derivative classification markings, see Finding 4.

Conclusions

We found that the Department needs to improve its review of classified documents to ensure that information is appropriately marked. Because all required markings were not included on the documents, an individual using these documents as a reference for a derivative classification decision may not have the necessary information to correctly mark the document. This could result in an over-classification, misclassification, or unauthorized release of classified information.

Recommendation 6 to the OCA

Correct the markings on the two originally classified documents so that it is clear that the documents are original classifications, not derivative classifications.

Agency Response

OHSEC will correct the markings by end of the first quarter of FY 2014.

OIG Position

We are unable to accept management decision at this time. The response states that OHSEC will correct the markings on the documents. However, OHSEC does not have original classification authority. Since the two documents were approved as original classifications by the OCA, this individual would have to approve any corrections by OHSEC on the documents.

In order to reach management decision, the response needs to specify that the OCA will review and approve any changes to the markings on the originally classified documents and provide an estimated completion date.

Recommendation 7 to PDSD

Develop and implement a checklist to be used by the OCA, at the time of classification, to ensure that all originally classified documents include the required markings.

Agency Response

OHSEC will develop a checklist by end of the first quarter in FY 2014.

OIG Position

We accept management decision for this recommendation.

Finding 4: Effectiveness of Derivative Classification Decisions and Dissemination Control Marking Decisions

Derivative classification means incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

We found that USDA personnel did not properly mark derivatively classified documents. Our review of 14 documents, derivatively classified between October 2010 and April 2013, found that 9 did not identify who was applying the markings, 8 did not carry forward the declassification date, and 7 did not contain the portion markings. These derivative classification markings were missing because staff misunderstood how to mark these documents and, instead, mistakenly treated them as working papers. Until staff are fully familiar with specific classified documents' marking requirements, USDA runs the risk of over-classifying or improperly releasing national security information.

The Federal regulation governing classified national security information details a uniform security classification system, which requires that standard markings be applied to classified information. Additionally, the regulation states that the markings of classified information shall not deviate, unless approved by the Director of ISOO. Markings must be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.[32] Derivatively classified documents must carry forward the markings from the source document or follow marking instructions in the appropriate classification guide.[33] The required markings of derivatively classified information are:

- "Classified By" – the identity of the person applying the derivative classification by name and position or personal identifier (if not evident, the agency and office of origin shall be identified and follow the name on the "Classify by" line).
- "Derived From" – the source of the information; if multiple sources, the marking can state "multiple sources," but a list must be included or attached (including the agency, office of origin, and the date of the source document or guide).
- "Declassify On" – the declassification date will be carried forward from the source document or the duration instruction from the classification guide; however, if multiple source documents are used, then the longest duration of any of its source documents is used.
- Overall classification – the highest level of classification of information contained within the document, placed conspicuously at the top and bottom of the outside front cover (if any), on the title page (if any), on the top and bottom of every page, and on the outside of the back cover (if any).

[32] 32 CFR 2001.20, July 1, 2010 Edition.
[33] 32 CFR 2001.22(a), July 1, 2010 Edition.

- Portion markings – each portion of a derivatively classified document shall be marked immediately preceding the portion to which it applies, in accordance with its source document.
- Date of origin of document – the date of origin of the document must be indicated in a manner that is immediately apparent.
- Dissemination control and handling markings – additional control and handling markings that supplement the overall classification markings, if required by the agency.[34]

The only exception to these requirements is for a working paper. Working papers are defined as documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention. If a document or material is expected to be released by the originator outside of the originating activity, retained for more than 180 days from date of origin, or filed permanently, then it must be portion marked in the same manner as described for a finished document.[35]

We reviewed a total of 14 derivatively classified documents within the scope of our review (October 2010 through April 2013). Of the 14, 9 were briefing documents[36] (one of which was classified as Top Secret–sensitive compartmented information). We found that none of the nine briefing documents contained all the required markings. While all the briefing documents were marked with the overall marking of Secret or Top-Secret, they did not contain all of the remaining required elements, such as who classified the document, the source of the information, when it was to be declassified, or the portion markings. Therefore, those that received the briefing would not know what parts of the documents were unclassified, making such portions of the briefings over-classified.

Based on our review, we determined that staff misunderstood how to handle briefing documents, due to insufficient training and guidance (For additional issues on training, see Finding 7). One person interviewed believed that if the presentation was not going to be maintained longer than 180 days (working paper retention period), it did not need all the markings. As the briefing documents were not meant to be maintained, the individual saw these as working papers. As a working paper, the briefing documents would be considered "draft" documents, not to be released by the originator, and portion marking would not be required. However, because the documents were used for presentation and released outside of the originating activity, the required markings must be applied. An agency official confirmed that these documents were improperly marked. He further stated that when briefing documents are presented to individuals outside the agency, the proper markings must be applied.

Conclusions

We found that because personnel were not sufficiently aware that briefing documents containing classified information are not to be treated as working papers, these briefing documents did not

[34] 32 CFR 2001.22(b-i), July 1, 2010 Edition.
[35] 32 CFR 2001.24(d), July 1, 2010 Edition.
[36] The documents consisted of briefing slides.

receive all the necessary markings. While a derivative classifier referred to these missing elements as "administrative errors," these errors could result in over-classification of information. It is therefore crucial that all staff who are responsible for marking these documents have an understanding of the various classified documents and their particular marking requirements and that the Department take steps to ensure that its documents are properly marked.

Recommendation 8 to PDSD

Develop and conduct specialized training for derivative classifiers that discusses the differences between working papers and finished documents and the marking requirements, as described in the regulation.

Agency Response

OHSEC will deliver specialized training for derivative classifiers by the end of the second quarter of FY 2014.

OIG Position

We accept management decision for this recommendation.

Recommendation 9 to PDSD

Coordinate with the subordinate agencies to review all USDA classified documents maintained, and correct all improper markings identified.

Agency Response

OHSEC will lead a review process with all subordinate agencies to review and correct all USDA classified documents as needed by the end of FY 2014.

OIG Position

We accept management decision for this recommendation.

Finding 5: Effectiveness of Security Self-Inspection Program

The SAO is required to establish a self-inspection program and report annually on it to the Director of ISOO. We determined that USDA does not ensure that its subordinate agencies are conducting self-inspections in accordance with regulations and procedures. We also found that the program was ineffective at providing information about the structure and implementation of USDA's self-inspection program and reporting on the findings from this program. This occurred because PDSD Information Security staff do not follow up with subordinate agencies to obtain and maintain adequate documentation of self-inspections subordinate agencies have conducted (See Finding 6). Therefore, USDA is unable to effectively track the findings or recommendations for improvement that resulted from the self-inspections conducted by its subordinate agencies. Additionally, USDA does not have complete information summarizing the results of its self-inspection program, which is necessary to adequately determine the effectiveness of its classified national security information program within individual agency activities and the Department as a whole.

E.O. 13526[37] and the Federal regulation[38] require SAOs to establish self-inspection programs. According to USDA's Departmental manual, self-inspections should be completed a minimum of every 2 years by agencies that receive, generate, and store classified information. Copies of the inspection report must be sent within 5 calendar days to PDSD for record purposes. The report should also be forwarded to senior agency management for their overall program security awareness and to assist them in planning for future security upgrades or expenses. E.O. 13526 and the Federal regulation[39] also require SAOs to report annually on their self-inspection program to the Director of ISOO. The report provides information about the structure and implementation of the agency's self-inspection program and identifies the findings from this program, which has been established by the SAO to help oversee the agency's classified national security information program.

The information contained in the self-inspection report(s) should flow as follows: The first part of the report is a description of the agency's self-inspection program that outlines how the program addresses the requirements of the regulation.[40] The second part is an account of the findings of the agency's self-inspection program. This must include an assessment and summary of the findings and specific information about the review of the agency's original and derivative classification actions. Also, it is essential that the report identify corrective actions that have been taken or are planned to address deficiencies and misclassification actions. Lastly, if best practices were identified during the self-inspections, they should be included in the report as well.

Because PDSD Information Security staff do not maintain documentation of the self-inspections, OIG was unable to verify that subordinate agencies performed self-inspections. USDA reported to ISOO on the *Agency Security Classification Management Program Data Report* (Standard

[37] 75 FR 707, section 5.4(d)(4), January 5, 2010.
[38] 32 CFR 2001.60(b), July 1, 2010 Edition.
[39] 32 CFR 2001.60(f)(2), July 1, 2010 Edition.
[40] 32 CFR 2001.60(a-e), July 1, 2010 Edition.

Form (SF)-311) that 10, 3, and 13 self-inspections had been conducted in FYs 2010, 2011, and 2012, respectively. However, when requested by OIG, the Information Security staff were only able to provide documentation to support three self-inspections performed in FY 2012 (See Finding 6).

The documentation of self-inspections is necessary in order for PDSD to track findings and determine whether corrective action has been taken. Without these self-inspection reports, OIG was unable to review findings or corrective actions from the remaining 23 self-inspection reports and concluded that the self-inspection program was ineffective. The staff agreed that improvement is needed in the documentation of the self-inspection program.

We also noted problems with how USDA was reporting to ISOO on the Department's self-inspection program (See Finding 6). We reviewed the reports from the previous 2 fiscal years and noted that required information was not provided to ISOO. Specifically, the USDA's FY 2011 annual self-inspection report did not include the following information:

- A description of the agency's self-inspection program to include activities assessed, program areas covered, and methodology utilized.
- An assessment and a summary of the findings of the agency's self-inspection program in the following program areas: original classification, derivative classification, declassification, safeguarding, security violations, and management and oversight.
- Specific information with regard to the findings of the annual review of the agency's original and derivative classification actions to include the volume of classified materials reviewed and the number and type of discrepancies identified.
- Actions that have been taken or are planned to correct identified program deficiencies, marking discrepancies, or misclassification actions, and to deter their reoccurrence.
- Best practices that were identified during self-inspections.

Similar deficiencies were noted in the FY 2012 annual self-inspection report. This report did not include the following information:

- A description of the agency's self-inspection program to include activities assessed, program areas covered, and methodology utilized.
- An assessment and a summary of the findings of the agency's self-inspection program in the following program areas: derivative classification and security violations.
- Specific information with regard to the findings of the annual review of the agency's derivative classification actions to include the volume of classified materials reviewed and the number and type of discrepancies identified.
- Best practices that were identified during self-inspections.

PDSD staff stated that, while they try to gather the missing information, due to resource constraints, they allow the subordinate agencies to complete the self-inspection and send in their results to PDSD. They acknowledged that in some cases, they may not have received all the self-inspections (See Finding 6).

Also, ISOO conducted a review of USDA's classified national security information program in 2005 and found a high percentage of classified documents with marking errors, which indicated USDA's prior corrective actions were not adequate to eliminate future marking errors.[41]

Conclusions

Self-inspections can be a valuable guide to pinpointing deficiencies and effectively addressing them. If the self-inspection program is not gathering the necessary information, or the self-inspections are not performed regularly and as required, the self-inspection program's impact will be greatly weakened and the issues will persist. For instance, in 2005, ISOO reported a high percentage of classified documents with marking errors. A self-inspection program, which includes the requirements for marking classified documents, that is efficiently conducted and documented, could assist PDSD in identifying and addressing continued issues regarding marking errors (See Findings 3 and 4).

Because ISOO relies on the information agencies report to determine the status of the classification programs in both Government and industry on an annual basis, it is essential that USDA ensures it is reporting complete information. Without proper documentation of a self-inspection program, and reporting of essential security information to ISOO, USDA is unable to ensure that it has an effective classified national security information program.

Recommendation 10 to the SAO

Direct all subordinate agencies to schedule, conduct, and document self-inspections and provide the completed inspections to PDSD.

Agency Response

As answered in Recommendation 9, OHSEC will coordinate with subordinate agencies to schedule, conduct, and document self-inspections by the end of FY 2014.

OIG Position

We accept management decision for this recommendation.

Recommendation 11 to the SAO

Develop and implement procedures that require PDSD to report to the SAO on the completion of the subordinate agency self-inspections.

[41] ISOO *Report of On-site Review and Document Review of USDA*, December 5, 2005.

Agency Response

Currently, the SAO has provided a response through the required SF-311 reporting process. This process will be updated by the end of the first quarter FY 2014 to ensure all SF-311 reports are submitted to the SAO or their designee prior to being submitted to ISOO.

OIG Position

We are unable to accept management decision at this time. The response stated that the process will be updated to ensure that all SF-311s are provided to the SAO or designee before being provided to ISOO. However, the recommendation requires PDSD to report to the SAO on the completion of the subordinate agency self-inspections, not completing the SF-311s, which was addressed in Finding 6.

In order to reach management decision, the response needs to specify that a procedure will be developed that requires PDSD to report to the SAO on the completion of the subordinate agency self-inspections and provide an estimated completion date for implementation of the procedure by the SAO.

Recommendation 12 to the OCA

Develop and implement procedures that require the SAO to review and verify that the annual self-inspection report includes all required information, prior to submitting the report to ISOO.

Agency Response

As identified in Recommendation 11, this process will be updated by the end of the first quarter of FY 2014.

OIG Position

We are unable to accept management decision at this time. The response did not address the development of procedures to require the SAO to verify that all required information was included in the annual self-inspection report. Instead, the response discussed a different report, the SF-311 that is provided to ISOO.

In order to reach management decision, the response needs to specify that the procedure will be developed and provide an estimated completion date for implementation of the procedure by the OCA.

Finding 6: Effectiveness of Security Reporting

Each agency, e.g., USDA, is required to gather information and report on the state of its security program. We found that USDA has not effectively gathered information and reported statistics related to its security classification program. This occurred because USDA's subordinate agencies do not always provide PDSD with reports containing the needed information or documentation. As a result, ISOO may be receiving and relying upon incomplete or inaccurate information concerning the status of USDA's security classification program.

According to Federal regulation,[42] each agency that creates or safeguards classified information must annually report to the Director of ISOO statistics related to its security classification program by using the *Agency Security Classification Management Program Data Report* (SF-311). The SF-311 is a data collection form completed only by those Executive branch agencies that create and/or handle classified national security information.

To meet these requirements, each USDA subordinate agency must annually complete an individual SF-311 and submit it to PDSD. PDSD Information Security staff then compile this information into a comprehensive SF-311. PDSD submitted the comprehensive forms to ISOO for FYs 2010, 2011, and 2012, on behalf of USDA.

If subordinate agencies have not submitted their reports, the agency (USDA) may request an extension from ISOO or submit the comprehensive SF-311, with an annotation stating which subordinate agencies did not submit their reports, and ISOO will note this in the annual report. Additionally, if an agency estimates the number of derivative classification decisions, the sampling period and multiplier used shall be annotated in the comments section of the SF-311.

We found that USDA's comprehensive SF-311s submitted to ISOO contained unsupported data that, at times, conflicted with the data submitted in the subordinate agencies' SF-311s. For example, in FY 2011, USDA reported 531 derivative classification decisions, but the SF-311s provided by subordinate agencies supported only 103. Similarly, in FY 2012, USDA reported 7,179 derivative classification decisions, while subordinate agencies' SF-311s supported only 6,439.

We also found that USDA's comprehensive reports to ISOO did not always accurately reflect the number of self-inspections reported by subordinate agencies. The table below presents the number of self-inspections reported to both ISOO and PDSD for FYs 2010, 2011, and 2012.

FY	Number of Self-Inspections Reported to ISOO	Number of Self-Inspections Reported to PDSD
2010	10	10
2011	3	10
2012	13	7

[42] 32 CFR 2001.90(b), July 1, 2010 Edition.

PDSD Information Security staff stated that these variances occurred because not all subordinate agencies responded to PDSD's annual request for data, and PDSD did not have the ability to enforce compliance. OIG found that USDA does not have guidance in place directing subordinate agencies to annually submit the required statistical information. PDSD Information Security staff further explained that, because subordinate agencies do not always provide statistical information to PDSD, PDSD must often contact each subordinate agency individually to obtain the required data. PDSD Information Security staff may then adjust the numbers based on the verbal contact and their own knowledge of the agency's classified national security information activity for the year.

We found that PDSD did not document in the SF-311 comments section how it calculated estimated statistics. Additionally, when requested, PDSD staff were unable to determine how the calculation was performed and could not provide documentation for the basis of the estimate. This occurred primarily because PDSD does not have procedures in place to document the statistical information it receives, or to document any changes or estimations of this information.

OIG noted that USDA may request to extend its deadline in order to have more time to follow up with subordinate agencies. Additionally, USDA must notify ISOO which subordinate agencies did not report, so that ISOO can include this information in the annual report. Finally, when estimating numbers and statistics, PDSD should document and explain its methodology for doing so in the comments section when submitting this information to ISOO, as required.

Conclusions

PDSD can improve the accuracy of its annual report (SF-311) if it obtains information from all subordinate agencies and it fully documents methodologies for estimating information. While OIG acknowledges that individual followup can be lengthy and time-consuming, requesting extensions, as well as reporting which subordinate agencies did not provide information, will increase the likelihood of subordinate agencies providing accurate information. Additionally, USDA must have clear procedures and direction for both PDSD and subordinate agencies on how to document the numbers they report. USDA must ensure that it is submitting accurate information to ISOO, since this information is crucial to ensuring the effectiveness of statistical reporting.

Recommendation 13 to the SAO

Direct all subordinate agencies to provide required statistical information to PDSD annually to ensure accurate reporting to ISOO.

Agency Response

Additional direction will be provided to the subordinate agencies outlining the requirement to provide annual reporting by the end of the first quarter of FY 2014.

OIG Position

We accept management decision for this recommendation.

Recommendation 14 to PDSD

Develop procedures to fully document the statistical information (including methodologies utilized for changing or estimating data) used to support the annual report to ISOO.

Agency Response

OHSEC will develop procedures to document the information by the end of the second quarter of FY 2014.

OIG Position

We accept management decision for this recommendation.

Finding 7: Effectiveness of Security Education and Training

PDSD's classification management training content and documentation need to be improved on a more general level, particularly in providing required information to individuals with security clearances. Specifically, we found that PDSD does not maintain records of the training provided outside of AgLearn,[43] and the training documents for the Classified National Security Information Annual Refresher Briefing did not cover all the required elements of the biennial training. This occurred because the training records management system is inadequate, and training documents have not been updated to cover all required topics. As a result, there is a greater risk that individuals creating or handling classified information have not been adequately trained to do so. This may result in over-classification, misclassification, or improper release of national security information.

According to Federal regulation, all executive branch employees who create, process, or handle classified information must undergo training. All agencies are to conduct training tailored to the organization, using briefings, interactive videos, dissemination of instructional materials, online presentations, or other methods, and maintain records about the training and the employees who participated in the training.[44]

OCAs are required to receive training before classifying original information and then at least once each calendar year thereafter. The annual training must include guidance on proper classification and declassification procedures, with an emphasis on the avoidance of over-classification. Everyone who applies derivative classification markings is to receive training on proper application of the derivative classification principles before classifying information, and retraining at least once every 2 years.

The biennial training for derivative classifiers must include:

- principles of derivative classification;
- classification levels;
- duration of classification;
- identification and markings;
- classification prohibitions and limitations;
- sanctions;
- classification challenges;
- security classification guides; and
- information sharing.

[43] The Agriculture Learning (AgLearn) system is USDA's Departmentwide system for managing training records and activity at USDA.
[44] 32 CFR 2001.70, July 1, 2010 Edition.

The regulation also states that the penalty for not completing the mandatory training for either an OCA or a derivative classification authority (DCA) is a suspension of the individual's authority until the training is completed.[45]

We found that USDA's current training efforts need improvement to meet these requirements. USDA incorporated the required biennial training for DCAs with its annual refresher on security education and training through the online training system AgLearn. The agency stated that this training was given to everyone who holds a security clearance that gives them the authority to handle, create, or process classified information. We reviewed training records for 128 of these individuals to verify they had received training and that the training received met the requirements for possible derivative classifiers.[46]

We found that the USDA's training program and retention of training records was not in accordance with ISOO's regulations and the E.O., and lacked key information. Specifically, the AgLearn training did not cover:

- avoidance of over-classification;
- prohibitions and limitations on classification;
- classification challenges; and
- information sharing.

In addition to not covering the above elements, the AgLearn training did not clearly address:

- principles of derivative classification;
- duration of classification; and
- classification guides.

As a result, the USDA employees who took the training through AgLearn were not properly trained in all aspects of derivative classification.

PDSD also did not keep sufficient documentation to support that all Secure Network (SN) users completed the training. This had been an issue which ISOO reported in 2005. We found that of the 128 SN users, PDSD did not have records showing that 28 of these users completed the training through AgLearn. Furthermore, PDSD could not provide evidence that the OCA had received the required annual training. Additionally, while PDSD officials stated that anyone who could not complete the training in AgLearn did so through an alternative process, they were able to provide documentation supporting that only 9 of the 28 users had completed training through this process. Therefore, 19 of the 128 SN users may not have received the required training.

---

[45] 32 CFR 2001.71(c)(3)(i-ii) states that "[a]n agency head, deputy agency head, or senior agency official may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers shall be documented. Whenever such a waiver is granted, the individual shall receive the required training as soon as possible."

[46] These individuals were identified by PDSD as having Secure Network (SN) accounts. Individuals within USDA that have an SN account could potentially create a derivatively classified document because classified information can only be processed on a certified and accredited computer system.

PDSD officials stated that they did not waive the training requirement for those who could not complete the training for various reasons. However, PDSD does provide extensions for completing the training on a case-by-case basis, such as when a user was on military orders, AgLearn was not working, or users were unable to access AgLearn from their location. When asked about suspending an original or derivative classifier's authority to classify, as required by the regulation, PDSD officials stated that there were no suspensions.

Conclusions

PDSD needs to take further steps to ensure that all personnel who handle, create, and process classified information receive adequate training. This requires training content that comprehensively covers all requirements, and a method of documenting which personnel have received such training. Training is necessary to ensure that the OCA and DCAs have satisfactory knowledge and understanding of classification, safeguarding, and declassification of national classified information. Training also increases uniformity and reduces over-classification or improper classification, improper safeguarding, and inappropriate or inadequate declassification practices. Because PDSD does not waive the training requirement or suspend anyone's authority to classify information, it must maintain records of training for everyone within USDA who has a security clearance.

Recommendation 15 to PDSD

Develop, complete, and record computer-based training (AgLearn) that meets all the requirements for the original and derivative classification authorities.

Agency Response

OHSEC is currently updating the FY 2014 computer-based training, and requirements will be met by the end of FY 2014.

OIG Position

We accept management decision for this recommendation.

Recommendation 16 to PDSD

Establish a tracking system to record and manage training completed outside of AgLearn for everyone with original or derivative classification authorities.

Agency Response

USDA considers AgLearn the authoritative tool for providing training and education to its employees on a myriad of subject matter that is conducive to their personal and professional development. OHSEC utilizes this methodology to reach the estimated 3,500 cleared staff

within all of the agencies that comprise USDA and considers the completion reports that come from AgLearn as an authoritative document.

OIG Position

We are unable to accept management decision at this time. The response did not provide a method to record training for those individuals who are not able to complete it in the AgLearn system and therefore must complete it in an alternative manner.

In order to reach management decision, OHSEC needs to develop a process to record and manage training for those individuals who are not able to access the AgLearn system and must complete it through an alternative method and provide an estimated completion date.

Recommendation 17 to PDSD

Develop procedures that identify those original or derivative classification authorities who do not complete required training annually or biennially, as appropriate, and suspend those individuals' authority to classify information, until training is completed.

Agency Response

OHSEC will recommend suspension for anyone who does not complete their training and who does not have approval for an exemption.

OIG Position

We are unable to accept management decision at this time. OHSEC stated that it will recommend suspension for anyone who does not complete their training but did not include procedures that will be developed to suspend individuals.

In order to reach management decision, OHSEC needs to specify the actions planned or completed to develop procedures to identify and address those individuals who do not complete the required training and suspend those individuals' authority along with an estimated completion date.

Scope and Methodology

Our audit examined 31 documents classified by USDA at the "Secret" and "Top-Secret" level, either originally or derivatively (16 classified since October 1, 2010, and 15 classified prior to that date). We conducted fieldwork from February 2013 through July 2013. We conducted our audit by visiting OHSEC in Washington, D.C., as well as five locations that store classified national security information (four in Washington, D.C., and one storage location in Riverdale, Maryland).

We used a guide that was prepared by a working group of participating Inspectors General (IG), for all IG offices participating in this Governmentwide effort, on behalf of the Council of the Inspectors General on Integrity and Efficiency. The guide was developed to meet the requirements of Public Law 111-258, Reducing Over-Classification Act, regarding the responsibilities of each participating Department and agency. The IG working group was formed to ensure consistency in the evaluative process, comparable reporting, and the ability to compare results across agencies. As directed by the Act, we consulted with ISOO and coordinated throughout the evaluation with another IG office, with the intent of ensuring that our review followed a consistent methodology to allow for cross-agency comparisons. We were assisted during our review of determining the appropriateness of classification decisions by auditors from the Defense Intelligence Agency.

USDA did not maintain an inventory of all classified documents. To select documents for review, we first obtained a list of 128 individuals with Secure Network (SN) accounts from PDSD. This SN serves as a classified Automated Information System to provide cleared analysts the ability to communicate within the classified environment. This network is not a USDA information system; it is controlled and owned by another Federal Government agency. We did not evaluate the effectiveness of this information system or its controls, as the proper classification, declassification, and marking of classified national security information is manually controlled by the OCA and the DCA at the time a classification decision is made. As such, we did not rely upon an information system to obtain sufficient, appropriate evidence to support the findings presented in this report.

The list of individuals with SN accounts obtained included names and telephone numbers, as well as the individual's agency and office. Of the 128 SN users listed, one individual was removed from the list, due to retirement/transfer. Therefore, OIG sent 127 SN users a survey aimed at establishing the number of DCA decisions made since October 1, 2010. Of the 127 surveys sent out, 12 of the recipients were either out of the country, their account had been terminated after we were provided the listing, or they were on extended leave and no response was expected. Of the 115 individuals remaining, 90 responded to our survey. Based on the surveys received, eight individuals indicated they had made DCA decisions since October 1, 2010. We interviewed these 8 individuals, and were able to identify and review 14 DCA determinations made since October 1, 2010, and available for our review at the time the fieldwork was conducted. OIG also identified and reviewed two OCA determinations made since October 1, 2010. In addition, OIG selected 14 DCA documents and 1 OCA document outside the scope of the audit (prior to October 1, 2010) to evaluate whether the agency is proactive with its declassification procedures.

Our review focused on eight areas: original classification authority; general program management responsibilities; original classification; derivative classification; declassification; self-inspections; reporting and definitions; and security education and training.

To discern whether Departmental policies and practices were consistent with E.O. 13526 and 32 CFR 2001, we used the following tools developed by ISOO:

- an agency regulation implementing assessment tool;
- methodology for determining the appropriateness of an original classification decision;
- original classification authority interview coverage;
- methodology for determining appropriateness of a derivative classification decision; and
- derivative classifier interview coverage.

To further assess whether policies, procedures, rules, regulations, and practices had been adopted, followed, and effectively administered, as well as to identify policies and practices that may be contributing to persistent misclassification, we also:

- examined the results of the fundamental classification guidance review;
- examined the results of self-inspection reporting;
- examined Forms SF-311, "Agency Security Classification Management Program Data";
- reviewed relevant policies, regulations, and related studies;
- reviewed 31 classified documents;
- conducted a survey/questionnaire of original and derivative classifiers;
- interviewed two security managers, along with eight derivative classifiers; and
- interviewed key department officials responsible for security training and related policy development and implementation.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions, based on our objectives.

Abbreviations

AgLearn .....Agriculture Learning system
CFR ..... *Code of Federal Regulations*
DCA ..... Derivative Classification Authority
DM ..... Departmental Manual
DR ..... Departmental Regulation
E.O. ..... Executive Order
FR ..... *Federal Register*
FY ..... Fiscal Year
IG ..... Inspector General
ISC ..... Interagency Security Coordinator
ISCAP ..... Interagency Security Classification Appeals Panel
ISOO ..... Information Security Oversight Office
OCA ..... Original Classification Authority
OHSEC ..... Office of Homeland Security and Emergency Coordination
OIG ..... Office of Inspector General
PDSD ..... Personnel and Document Security Division
SAO..... Senior Agency Official
SF ..... Standard Form
SN ..... Secure Network
USDA..... U.S. Department of Agriculture

Exhibit A: Effectiveness of Classification Management Policies and Control Marking Guidelines

In the following table, the first column describes the requirement, the second column provides the citation source for the requirement, and the third column describes how USDA's current policy differs from the requirement shown in column one.

Criteria	Citation	USDA's Current Regulation and Manual
Original Classification Authority		
OCA was given to the Secretary of Agriculture who "may not delegate the authority" (see Finding 1).	75 FR 735-736	USDA's regulation and manual both state the Secretary "may re-delegate" OCA to the Deputy Secretary.
General Program Management		
OCAs and DCAs are suspended, until mandatory training requirements are met (see Finding 1).	75 FR 707, sections 1.3(d) and 2.1(d); and 32 CFR 2001.71(c)(3) and (d)(3)	Agency guidance does not provide a penalty (suspension) for not completing the required training.
Original Classification		
Original classification authority is classifying the information.	75 FR 707, section 1.1(a)(1)	Agency guidance does not cite the OCA classification standards.
If there is significant doubt about the need to classify information.	75 FR 707, section 1.1(b)	Agency guidance does not discuss the presumption against classification when doubt exists.
Classified addendum (see Finding 1).	75 FR 707, section 1.6(g)	The use of a classified addendum is not discussed in agency guidance.
Date of origin of document.	32 CFR 2001.21(e)	Agency guidance does not specify that the date of origin of a classified document must be applied to OCA documents.
Electronic environment markings for classified: e-mails, web pages, uniform resource locators (URL), databases, bulletin boards, wikis, instant messaging, and attached files.	32 CFR 2001.23	USDA's manual covered the marking of electronic external removable data storage device (use of label) and e-mails only (DM 3440-001, chapter 4, sections 4b(6) and 7).
Individuals must be advised of their right to appeal agency decisions to ISCAP (see Finding 1).	75 FR 707, section 1.8 (b)(3)	The manual does not advise individuals of this right.

Classification Challenges • initial written response to a challenge within 60 days. • if unable to respond to the challenge within 60 days, the agency must acknowledge the challenge in writing, and provide a date by which the agency will respond. • must include a statement that, if no agency response is received within 120 days, the challenger has the right to forward the challenge to ISCAP for a decision. • forward the challenge to ISCAP if an agency has not responded to an internal appeal within 90 days (see Finding 1).	32 CFR 2001.14(b)(3)	Agency guidance does not address these timeframes. The manual only addresses a 30-calendar day response from PDSD (DM 3440-001, chapter 2.1.f).
Classification guides shall conform to standards and be reviewed and updated.	75 FR 707, section 2.2(a and c)	Agency guidance does not contain procedures for the publication and updating of classification guides which meet the minimum standards.
Derivative Classification		
DCA needs to be identified by name and position, or by personal identifier (see Finding 1).	75 FR 707, section 2.1(b)(1); and 32 CFR 2001.22(b)	Agency guidance does not require the name or personal identifier of those who apply derivative classification markings.
Transmittal document markings.	32 CFR 2001.24(b)	Agency guidance does not discuss the required markings for transmittal documents.
Date of origin of document.	32 CFR 2001.22(i)	Agency guidance does not specify that the date of origin of a classified document must be applied to DCA documents.
Declassification		
Automatic Declassification.	75 FR 707, section 3.3; and 32 CFR 2001.30(m)	Agency guidance does not include procedures for processing requests to ISCAP for exemptions from automatic declassification.

An agency shall notify ISCAP of any specific file series of records that falls within one or more of the automatic declassification exemption categories.	75 FR 707, section 3.3; and 32 CFR 2001.30(n)(5)	Agency guidance does not include a process for file series exemptions.
Each agency shall publish in the *Federal Register* regulations concerning the handling of mandatory declassification.	32 CFR 2001.33(a)	Agency mandatory declassification procedures were not published in the *Federal Register*.
Self-Inspections		
SAO shall report annually to the Director of ISOO on the agency's self-inspection program. The report shall include: description of the agency's self-inspection program; assessment and a summary of the findings; specific information regarding the findings; the action taken; and best practices (see Finding 1).	75 FR 707, section 5.4(d)(4); 32 CFR 2001.60(f)(2); and 32 CFR 2001.90(d)	Agency guidance does not address the external reporting of self-inspections.
Regular reviews of representative samples of the agency's original and derivative classification actions shall encompass all agency activities that generate classified information.	32 CFR 2001.60(c)(2)	Agency guidance does not discuss reviewing representative samples of OCA and DCA documents and corrections of misclassifications.
Reporting and Definitions		
Each agency shall report annually to the Director of ISOO statistics related to its security classification program.	32 CFR 2001.90(b)	Agency guidance does not address statistical reporting.
Agencies shall report annually to the Director of ISOO regarding security violations and/or improper declassifications.	32 CFR 2001.91(a), and 32 CFR 2001.91(d)	Agency guidance does not require a report to the Director of ISOO regarding security violations and/or improper declassifications.
Definitions as provided in the E.O. and CFR	75 FR 707, section 6.1; and 32 CFR 2001.92	Agency guidance does not include all definitions in accordance with the EO and 32 CFR 2001.
An initial fundamental classification guidance review shall be completed no later than June 27, 2012, and at least once every 5 years thereafter.	32 CFR 2001.16(a)	Agency guidance does not address a fundamental classification guidance review.

Security Education and Training		
The agency may grant a waiver of the training requirement due to unavoidable circumstances. Waivers shall be documented and training should be taken as soon as practicable.	32 CFR 2001.71(c)(3), and 32 CFR 2001.71(d)(3)	Agency guidance does not cover the waiver process for delays in training.

USDA'S
OFFICE OF HOMELAND SECURITY AND EMERGENCY COORDINATION'S RESPONSE TO AUDIT REPORT

United States
Department of
Agriculture

Office of Homeland
Security and
Emergency
Coordination

1400 Independence
Avenue SW

Washington, DC
20250

September 19, 2013

Mr. Gil Hardin
Assistant Inspector General for Audit
Office of the Inspector General
Washington, D.C. 20250

Dear Mr. Hardin:

Thank you for your letter on August 5, 2013, regarding the Classification Management Inspection Response for fiscal year 2013, Audit Number: 61701-0001-32.

We have reviewed the official draft report on the subject audit. We appreciate the opportunity to provide responses on the findings and the suggested recommendations. We have included the proposed corrective actions to be implemented, including timeframes for completion in the attachment.

Should you need clarification or additional information, please contact Mr. Cody Allers, Chief, Personnel and Document Security Division at (202)720-7373 or at cody.allers@dm.usda.gov.

Sincerely,

/S/

Todd H. Repass, Jr.
Director
Office of Homeland Security
and Emergency Coordination

Attachments

Attachment
Audit number -61701-0001-32 Response

Finding 1: Effectiveness of Security Program Management

- **Recommendation 1 to the Personnel and Document Security Division (PDSD)**

  Establish a records management system to facilitate the release of information after declassification date.

  Agency Response, Corrective action:

  To ensure classified records are maintained OHSEC uses DR 3080-001 and E.O. 13526. The ISC will be made aware of their responsibility in maintaining a separate classified records management system to the extent possible. Training will be incorporated into the annual refresher and specific training for the ISC will enable the identification, preservation, and retirement of permanent records. The general awareness will be incorporated into the FY 2014 annual refresher training. ISC specific training will be developed and implemented in AgLearn for all ISC by the second quarter of 2014.

- **Recommendation 2 to PDSD**

  Review all documents in which the declassification date has passed, in accordance with the "Mandatory Review for Declassification."

  Agency Response, Corrective action:

  OHSEC will incorporate specific guidance into the ISC specific training that addresses the need to review all classified holdings for appropriate markings and control information by the end of the second quarter of FY2014. This training will include the proper marking elements to ensure all responsible understand the marking and control requirements.

- **Recommendation 3 to the Senior Agency Official (SAO)**

  Dedicate the resources to expedite the process of ensuring the Departmental Regulation and Manual, DR 3440-001 and DM 3440-001, are updated to reflect Federal requirements (E.O. 13526 and 32 CFR 2001).

  Agency Response, Corrective action:

  OHSEC has identified the update of the DM 3440-001 as a critical priority for FY2014.

Finding 2: Effectiveness of Original Classification Authorities

- **Recommendation 4 to PDSD**

  Update the classification guide to include a point of contact and specific date or event for declassification.

  Agency Response, Corrective action:

  OHSEC believes that further guidance from Information Security Oversight Office (ISOO) is required. OHSEC will provide ISOO's guidance to OIG during the first quarter of FY2014.

- **Recommendation 5 to PDSD**

  Develop and implement procedures to review and update the classification guide when regulatory changes occur to ensure future compliance.

  Agency Response, Corrective action:

  OHSEC will prepare a policy memorandum outlining the new procedures. The memorandum will be distributed by the end of the first quarter of FY2014.

Finding 3: Effectiveness of Original Classification Decisions and Dissemination Control Marking Decisions

- **Recommendation 6 to the Original Classification Authority (OCA)**

  Correct the markings on the two originally classified documents so that it is clear that the documents are original classifications, not derivative classifications.

  Agency Response, Corrective action:

  OHSEC will correct the markings by end of the first quarter of FY2014.

- **Recommendation 7 to PDSD**

  Develop and implement a checklist to be used by the OCA, at the time of classification, to ensure that all originally classified documents include the required markings.

  Agency Response, Corrective Action:

  OHSEC will develop a checklist by end of the first quarter in FY2014.

Finding 4: Effectiveness of Derivative Classification Decisions and Dissemination Control Marking Decisions.

- **Recommendation 8 to PDSD**

  Develop and conduct specialized training for derivative classifiers that discusses the differences between working papers and finished documents and the marking requirements, as described in the regulation.

  Agency Response, Corrective action:

  OHSEC will deliver specialized training for Derivative Classifiers by the end of the second quarter of FY2014.

- **Recommendation 9 to PDSD**

  Coordinate with the subordinate agencies to ensure that review of all USDA classified documents are maintained; and correct all improper markings identified, as needed.

  Agency Response, Corrective Action:

  OHSEC will lead a review process with all subordinate agencies to review and correct all USDA classified documents as needed by the end of FY2014.

Finding 5: Effectiveness of Security Self-Inspection Program

- **Recommendation 10 to the OCA**

  Direct all subordinate agencies to schedule, conduct, and document self-inspections. The completed inspections should be submitted to the Personnel and Document Security Division (PDSD).

  Agency Response, Corrective Action:

  As answered in recommendation number 9 OHSEC will coordinate with subordinate agencies to schedule conduct and document self inspections by the end of FY2014.

- **Recommendation 11 to SAO**

  Develop and implement procedures that require PDSD to report to the SAO on the completion of the subordinate agency self-inspections.

Agency Response, Corrective Action:

Currently, the SAO has provided a response through the required SF-311 Reporting process. This process will be updated by end the first quarter FY2014 to ensure all SF-311 reports are submitted to the SAO or their designee prior to being submitted to ISOO.

- **Recommendation 12 to OCA**

  Develop and implement procedures that require the SAO to review and verify that the annual self-inspection report includes all required information, prior to submitting the report to the Information Security Oversight Office (ISOO).

  Agency Response, Corrective action:

  As identified in number 11 this process will be updated by the end of first quarter of FY2014.

Finding 6: Effectiveness of Security Reporting

- **Recommendation 13 to OCA**

  Direct all subordinate agencies to provide required statistical information to PDSD annually to ensure accurate reporting to the Information Security Oversight Office (ISOO).

  Agency Response, Corrective Action:

  Additional direction will be provided to the subordinate agencies outlining the requirement to provide annual reporting by the end of the first quarter of FY2014.

- **Recommendation 14 to PDSD**

  Develop procedures to fully document (including methodologies used for changing or estimating data) the statistical information used to support the annual report to the Information Security Oversight Office (ISOO).

  Agency Response, Corrective Action:

  OHSEC will develop procedures to document the information by the end of the second quarter of FY2014.

Finding 7: Effectiveness of Security Education and Training

- **Recommendation 15 to PDSD**

  Develop, complete, and record computer-based training (AgLearn) that meets all the requirements for the original and derivative classification authorities.

  Agency Response, Corrective Action:

  OHSEC is currently updating the FY2014 computer base training and requirements will be met by the end of FY2014.

- **Recommendation 16 to PDSD**

  Establish a tracking system to record and manage training completed outside of AgLearn for everyone with original or derivative classification authority.

  Agency Response, Corrective Action:

  USDA considers AgLearn the authoritative tool for providing training and education to its employees on a myriad of subject matter that is conducive to their personal and professional development. OHSEC utilizes this methodology to reach the estimated 3500 cleared staff within all of the agencies that comprise USDA and considers the completion reports that come from AgLearn as an authoritative document.

- **Recommendation 17 to PDSD**

  Develop procedures that identify those original or derivative classification authorities who do not complete required training annually or biennially, as appropriate, and suspend those individual's authorization to classify information, until training is completed.

  Agency Response

  OHSEC will recommend suspension for anyone who does not complete their training and who does not have approval for an exemption.

To learn more about OIG, visit our website at
www.usda.gov/oig/index.htm

How To Report Suspected Wrongdoing in USDA Programs

Fraud, Waste and Abuse
e-mail: USDA.HOTLINE@oig.usda.gov
phone: 800-424-9121
fax: 202-690-2474

Bribes or Gratuities
202-720-7257 (24 hours a day)