

CFR section	Related section of E.O. 13526
2001.10 Classification standards .....	1.1, 1.4
2001.11 Original classification authority .....	1.3
2001.12 Duration of classification .....	1.5
2001.13 Classification prohibitions and limitations .....	1.7
2001.14 Classification challenges .....	1.8
2001.15 Classification guides .....	2.2
2001.16 Fundamental classification guidance review .....	1.9
2001.20 General .....	1.6
2001.21 Original classification .....	1.6(a)
2001.22 Derivative classification .....	2.1
2001.23 Classification marking in the electronic environment ...	1.6
2001.24 Additional requirements .....	1.6
2001.25 Declassification markings .....	1.5, 1.6, 3.3
2001.26 Automatic declassification exemption markings .....	3.3
2001.30 Automatic declassification .....	3.3, 3.7
2001.31 Systematic declassification review .....	3.4
2001.32 Declassification guides .....	3.3, 3.7
2001.33 Mandatory review for declassification .....	3.5, 3.6
2001.34 Referrals .....	3.3, 3.6, 3.7
2001.35 Discretionary declassification .....	3.1
2001.36 Classified information in the custody of private organi- zations or individuals.	none
2001.37 Assistance to the Department of State .....	none
2001.40 General .....	4.1
2001.41 Responsibilities of holders .....	4.1
2001.42 Standards for security equipment .....	4.1
2001.43 Storage .....	4.1
2001.44 Reciprocity of use and inspection of facilities .....	4.1
2001.45 Information controls .....	4.1, 4.2
2001.46 Transmission .....	4.1, 4.2
2001.47 Destruction .....	4.1, 4.2
2001.48 Loss, possible compromise, or unauthorized disclo- sure.	4.1, 4.2
2001.49 Special access programs .....	4.3
2001.50 Telecommunications, automated information systems, and network security.	4.1, 4.2
2001.51 Technical security .....	4.1
2001.52 Emergency authority .....	4.2
2001.53 Open storage areas .....	4.1
2001.54 Foreign government information .....	4.1
2001.55 Foreign disclosure of classified information .....	4.1(i)(2)
2001.60 Self-Inspections, General .....	5.4
2001.70 Security Education and Training, General .....	5.4
2001.71 Coverage .....	1.3(d), 2.1(d), 3.7(b), 4.1(b), 5.4(d)(3)
2001.80 Prescribed standard forms .....	5.2(b)(7)
2001.90 Agency annual reporting requirements .....	1.3(c), 5.2(b)(4), 5.4(d)(4), 5.4(d)(8)
2001.91 Other agency reporting requirements .....	1.3(d), 1.7(c)(3), 1.9(d), 2.1(d), 5.5
2001.92 Definitions .....	6.1

**Subpart B—Classification**

**§ 2001.10 Classification standards.**

*Identifying or describing damage to the national security.* Section 1.1(a) of the Order specifies the conditions that must be met when making classification decisions. Section 1.4 specifies that information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security. There is no requirement, at the time of the decision, for the original classification authority to prepare a written description of such damage.

However, the original classification authority must be able to support the decision in writing, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand pursuant to the Order or law.

**§ 2001.11 Original classification authority.**

(a) *General.* Agencies shall establish a training program for original classifiers in accordance with subpart G of this part.

(b) *Requests for original classification authority.* Agencies not possessing such authority shall forward requests to the

Director of ISOO. The agency head must make the request and shall provide a specific justification of the need for this authority. The Director of ISOO shall forward the request, along with the Director's recommendation, to the President through the National Security Advisor within 30 days. Agencies wishing to increase their assigned level of original classification authority shall forward requests in accordance with the procedures of this paragraph.

(c) *Reporting delegations of original classification authority.* All delegations of original classification authority shall be reported to the Director of ISOO. This can be accomplished by an initial submission followed by updates on a frequency determined by the senior agency official, but at least annually.

**§ 2001.12 Duration of classification.**

(a) *Determining duration of classification for information originally classified under the Order—(1) Establishing duration of classification.* Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, an original classification authority shall follow the sequence listed in paragraphs (a)(1)(i), (ii), and (iii) of this section when determining the duration of classification for information originally classified under this Order.

(i) The original classification authority shall attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity, and shall assign such date or event as the declassification instruction.

(ii) If unable to determine a date or event of less than 10 years, the original classification authority shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

(iii) If unable to determine a date or event of 10 years, the original classification authority shall assign a declassification date not to exceed 25

years from the date of the original classification decision.

(2) *Duration of classification of special categories of information.* The only exceptions to the sequence in paragraph (a)(1) of this section are as follows:

(i) If an original classification authority is classifying information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, the duration shall be up to 75 years and shall be designated with the following marking, "50X1-HUM;" or

(ii) If an original classification authority is classifying information that should clearly and demonstrably be expected to reveal key design concepts of weapons of mass destruction, the duration shall be up to 75 years and shall be designated with the following marking, "50X2-WMD."

(b) *Extending duration of classification for information classified under the Order.* Extensions of classification are not automatic. If an original classification authority with jurisdiction over the information does not extend the classification of information assigned a date or event for declassification, the information is automatically declassified upon the occurrence of the date or event.

(1) If the date or event assigned by the original classification authority has not passed, an original classification authority with jurisdiction over the information may extend the classification duration of such information for a period not to exceed 25 years from the date of origin of the record.

(2) If the date or event assigned by the original classification authority has passed, an original classification authority with jurisdiction over the information may reclassify the information in accordance with the Order and this Directive only if it meets the standards for classification under sections 1.1 and 1.5 of the Order as well as section 3.3 of the Order, if appropriate.

(3) In all cases, when extending the duration of classification, the original classification authority must:

(i) Be an original classification authority with jurisdiction over the information;