

**§ 5.49**

(3) Compliance would reveal information properly classified in the interest of national security;

(4) Compliance would reveal confidential commercial or financial information or trade secrets without the owner's consent;

(5) Compliance would reveal the internal deliberative processes of the Executive Branch; or

(6) Compliance would potentially impede or prejudice an on-going law enforcement investigation.

**§ 5.49 Prohibition on providing expert or opinion testimony.**

(a) Except as provided in this section, and subject to 5 CFR 2635.805, Department employees shall not provide opinion or expert testimony based upon information which they acquired in the scope and performance of their official Department duties, except on behalf of the United States or a party represented by the Department of Justice.

(b) Any expert or opinion testimony by a former employee of the Department shall be excepted from 5.49(a) where the testimony involves only general expertise gained while employed at the Department.

(c) Upon a showing by the requestor of exceptional need or unique circumstances and that the anticipated testimony will not be adverse to the interests of the United States, the appropriate Department official designated in § 5.44 may, consistent with 5 CFR 2635.805, in their discretion and with the concurrence of the Office of the General Counsel, grant special, written authorization for Department employees, or former employees, to appear and testify as expert witnesses at no expense to the United States.

(d) If, despite the final determination of the appropriate Department official designated in § 5.44, a court of competent jurisdiction or other appropriate authority orders the appearance and expert or opinion testimony of a current or former Department employee, that person shall immediately inform the Office of the General Counsel of such order. If the Office of the General Counsel determines that no further legal review of or challenge to the court's order will be made, the Department employee, or former em-

**6 CFR Ch. I (1-1-07 Edition)**

ployee, shall comply with the order. If so directed by the Office of the General Counsel, however, the employee, or former employee, shall respectfully decline to testify.

**APPENDIX A TO PART 5—FOIA/PRIVACY ACT OFFICES OF THE DEPARTMENT OF HOMELAND SECURITY**

I. For the following Headquarters components of the Department of Homeland Security, FOIA and Privacy Act requests should be sent to the Departmental Disclosure Office, Department of Homeland Security, Washington, DC 20528. The Headquarters components are:

**A**

Office of the Secretary  
Office of the Deputy Secretary  
Office of the Under Secretary for Management

**B**

Office of the General Counsel  
Office of the Inspector General  
Office of International Affairs  
Office of Legislative Affairs  
Office of Public Affairs  
Office of National Capital Region Coordination  
Office of Professional Responsibility  
Office for State and Local Government Coordination

**C**

Directorate of Border and Transportation Security  
Directorate of Emergency Preparedness and Response  
Directorate of Information Analysis and Infrastructure Protection  
Directorate of Science and Technology

II. Requests made to components that have transferred or will transfer into the Department of Homeland Security, should be sent as follows:

A. Former components of the Department of Agriculture:

1. Animal and Plant Health Inspection Service, USDA, APHIS, LPA, FOIA, 4700 River Road, Unit 50, Riverdale, MD 20737-1232
2. Plum Island Animal Disease Center; Submit request to the APHIS address above or, FOIA Coordinator, USDA-REE-ARS-Information Staff, 5601 Sunnyside Avenue, Bldg. 1, Room 2248, Mail Stop 5128, Beltsville, MD 20705-5128

B. Former components of the Department of Commerce:

1. Critical Infrastructure Assurance Office (A former office of the Bureau of Industry and Security); Freedom of Information Coordinator, Bureau of Industry and Security,

## Office of the Secretary, DHS

## Pt. 5, App. A

Room 6883, U.S. Department of Commerce, Washington, DC 20230

2. FIRESTAT (formerly the Integrated Hazard Information System of the National Oceanic and Atmospheric Administration), National Oceanic and Atmospheric Administration, Public Reference Facility (OFAx2), 1315 East-West Highway (SSMC3), Room 10703, Silver Spring, MD 20910

C. Former components of the Department of Defense:

1. National Communications Service (A former component of the Defense Information Systems Agency), Defense Information Systems Agency, ATTN: RGC/FOIA Officer, 701 S. Courthouse Rd., Arlington, VA 22204-2199

D. Former components and programs of the Department of Energy:

The address for each component and program listed below is: U.S. Department of Energy, 1000 Independence Avenue, SW., Washington, DC 20585

1. Energy Assurance Office
2. Environmental Measurements Laboratory
3. Nuclear Incident Response Team
4. The chemical and biological national security and supporting programs and activities of the non-proliferation and verification research and development program.
5. The life sciences activities related to microbial pathogens of Biological and Environmental Research Program.
6. The nuclear smuggling programs and activities within the proliferation detection program of the non-proliferation and verification research and development program.
7. The nuclear assessment program and activities of the assessment, detection, and cooperation program of the international materials protection and cooperation program, and the advanced scientific computing research program and activities at Lawrence Livermore National Laboratory.
8. National Infrastructure Simulation and Analysis Center

E. Former components of the Department of Health and Human Services:

1. The address for each component and program listed below is: Department of Health and Human Services, Freedom of Information Officer, Room 645-F, Hubert H. Humphrey Building, Independence Avenue, SW., Washington, DC 20201;
  - a. Metropolitan Medical Response System,
  - b. National Disaster Medical System, and
  - c. Office of Emergency Preparedness
  - d. Strategic National Stockpile
2. Centers for Disease Control and Agency for Toxic Substances and Disease Registry, Attn: FOI Office, MS-D54, 1600 Clifton Road, NE., Atlanta, GA 30333.

F. Former components of the Department of Justice:

1. Immigration and Naturalization Service, Director, Freedom of Information/Privacy Act Program, Department of Justice, 425 Eye Street, NW., 2nd Floor, ULLICO Building, Washington, DC 20536 (for field offices, consult your phone book).

2. The address for each component and program listed below is: Federal Bureau of Investigation, Chief, FOIPA Section, 935 Pennsylvania Avenue, NW., Department of Justice, Washington, DC 20535-0001;

- a. National Infrastructure Protection Center,
- b. National Domestic Preparedness Office, and
- c. Domestic Emergency Support Team.

3. Office of Domestic Preparedness, U.S. Department of Justice, Office of Justice Programs, Office of the General Counsel, Attention: FOIA Staff, 810 7th Street, NW., Room 5400, Washington, DC 20531.

G. Former components of the Department of State:

Visa Office, Information and Privacy Coordinator, Office of Information Resources, Management Programs and Services, A/RPS/IPS, SA-2, Department of State, Washington, DC 20522-6001, Re: Freedom of Information Act Request.

H. Former components of the Department of Transportation:

1. Federal Aviation Administration, National Freedom of Information Act Staff, ARC-40, 800 Independence Avenue, SW., Washington, DC 20591 (for regional centers, consult your phone book).
2. Transportation Security Administration, TSA-1, FOIA Division, 400 Seventh Street, SW., Washington, DC 20590
3. United States Coast Guard, HQ USCG Commandant, G-CIM, 2100 Second Street, SW., Washington, DC 20593-0001 (for district offices, consult your phone book).

I. Former components of the Department of Treasury:

1. Federal Law Enforcement Training Center, Freedom of Information Act Officer, Townhouse 389, Glynco, GA 31524
2. U.S. Customs Service, Freedom of Information Act Request, Mint Annex, 1300 Pennsylvania Avenue, NW., Washington, DC 20229 (for field offices, consult your phone book).
3. U.S. Secret Service, Freedom of Information Act Request, 950 H Street, NW., Suite 3000, Washington, DC 20223, e-mail [FOIA@USSS.Treas.gov](mailto:FOIA@USSS.Treas.gov). Appeals should be addressed to the Deputy Director, United States Secret Service, Freedom of Information and Privacy Act Appeal Officer, at these same contact points.

J. Federal Emergency Management Agency: Federal Emergency Management Agency, Office of General Counsel, 500 C Street, SW., Room 840, Washington, DC 20472 (for regional offices, consult your phone book).

K. Former components of the General Services Administration:

1. For the Federal Computer Incident Response Center and the Federal Protective Service: Chief, FOIA Information Management Branch, GSA (CAIM), 1800 F Street, NW., Washington, DC 20405 (for regional offices, consult your phone book).

#### APPENDIX B TO PART 5—PUBLIC READING ROOMS OF THE DEPARTMENT OF HOMELAND SECURITY

The Headquarters components of the Department of Homeland Security do not maintain a conventional public reading room. Records that are required to be in the public reading room are available electronically at <http://www.dhs.gov/FOIA>.

Entities that will transfer into the Department of Homeland Security maintain public reading rooms as follows:

1. Former components of the Department of Agriculture:

Animal and Plant Health Inspection Service Library, 4700 River Road, Riverdale, MD 20737-1232

Plum Island Animal Disease Center, the APHIS address above or, USDA-ARS, 5601 Sunnyside Avenue, Building 1, Room 2248, Beltsville, MD 20705-5128

2. Former components of the Department of Commerce:

The Critical Infrastructure Assurance Office (A former office of the Bureau of Industry and Security) does not maintain a conventional public reading room. Records that are required to be in the public reading room are available electronically at <http://www.bis.doc.gov/FOIA/Default.htm>

FIRESTAT (formerly the Integrated Hazard Information System of the National Oceanic and Atmospheric Administration), NOAA Public Reference Facility, 1305 East-West Highway (SSMC4), Room 8627, Silver Spring, MD 20910

3. Former components of the Department of Defense:

The National Communication Service (A former component of the Defense Information Systems Agency) does not maintain a conventional public reading room. Records that are required to be in the public reading room are available electronically at <http://disa.mil/gc/foia/foia.html>

4. Former components and programs of the Department of Energy:

The address for each component and program listed below is: U.S. Department of Energy; 1000 Independence Avenue, SW., Washington, DC 20585

Energy Assurance Office  
Environmental Measurements Laboratory  
Nuclear Incident Response Team

The chemical and biological national security and supporting programs and activities of the non-proliferation and verification research and development program.

The life sciences activities related to microbial pathogens of Biological and Environmental Research Program.

The nuclear smuggling programs and activities within the proliferation detection program of the non-proliferation and verification research and development program.

The nuclear assessment program and activities of the assessment, detection, and cooperation program of the international materials protection and cooperation program, and the advanced scientific computing research program and activities at Lawrence Livermore National Laboratory.

The National Infrastructure Simulation and Analysis Center

5. Former components of the Department of Health and Human Services:

For the Metropolitan Medical Response System, the National Disaster Medical System, and the Office of Emergency Preparedness please contact the Freedom of Information Act Officer at: Department of Health and Human Services, Freedom of Information Officer, Room 645-F, Hubert H. Humphrey Building, Independence Avenue, SW., Washington, DC 20201

Strategic National Stockpile, Centers for Disease Control and Agency for Toxic Substances and Disease Registry, 1600 Clifton Road, NE., Room 4103, Building 1, Atlanta, GA 30333

6. Former components of the Department of Justice:

Immigration and Naturalization Service, 111 Massachusetts Avenue, NW., 2nd Floor, ULLICO Building, Washington, DC 20536

For the National Infrastructure Protection Center, the National Domestic Preparedness Office, and the Domestic Emergency Support Team: Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW., Department of Justice, Washington, DC 20535-0001

Office of Domestic Preparedness, U.S. Department of Justice, Office of Justice Programs, 810 7th Street, NW., Room 5430, Washington, DC 20531

7. Former components of the Department of State:

Visa Office, Department of State, 2201 C Street, NW., Washington, DC 20520

8. Former components of the Department of Transportation:

Federal Aviation Administration, 800 Independence Avenue, SW., Washington, DC 20591  
Transportation Security Administration, 400 Seventh Street, SW., Washington, DC 20590

United States Coast Guard Headquarters, 2100 Second Street, SW., Washington, DC

20593-0001 (for district offices, consult your phone book).

9. Former components of the Department of Treasury:

The Federal Law Enforcement Training Center does not maintain a conventional public reading room. Records that are required to be in the public reading room are available electronically at <http://www.fletc.gov/irm/foia/readingroom.htm>

U.S. Customs Service, 1300 Pennsylvania Avenue, NW., Washington, DC 20229 (for a list of field office public reading rooms please consult 19 CFR 103.1).

U.S. Secret Service, Main Treasury, 1500 Pennsylvania Avenue, NW., Washington, DC 20220

10. Federal Emergency Management Agency:

Federal Emergency Management Agency, Federal Center Plaza, 500 C Street, SW., Room 840 Washington, DC 20472 (for regional offices, consult your phone book)

11. Former components of the General Services Administration:

For the Federal Computer Incident Response Center and the Federal Protective Service: Central Office, GSA Headquarters, 1800 F Street, NW., (CAI), Washington, DC 20405 (for regional offices, consult your phone book).

#### APPENDIX C—DHS SYSTEMS OF RECORDS EXEMPT FROM THE PRIVACY ACT

This Appendix implements provisions of the Privacy Act of 1974 that permit the Department of Homeland Security (DHS) to exempt its systems of records from provisions of the Act. During the course of normal agency operations, exempt materials from other systems of records may become part of the records in these and other DHS systems. To the extent that copies of records from other exempt systems of records are entered into any DHS system, DHS hereby claims the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions in accordance with this rule.

Portions of the following DHS systems of records are exempt from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552(j) and (k):

1. DHS/ALL 001, Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System allows the DHS and its components to maintain and retrieve FOIA and Privacy Act files by personal identifiers associated with the persons submitting requests for information under each statute. Pursuant to exemptions (j)(2), (k)(1), (k)(2) and (k)(5) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H) and (I) and (f). Exemptions from the par-

ticular subsections are justified, on a case by case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension, which undermines the entire system.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of DHS or another agency. Access to the records would permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. The information contained in the system may also include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information also could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced, occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective enforcement of federal laws, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (H) and (I) (Agency Requirements), and (f) (Agency Rules), because portions of this system are exempt from the access provisions of subsection (d).

2. DHS-CRCL-001, Civil Rights and Civil Liberties Matters, which will cover allegations of abuses of civil rights and civil liberties that are submitted to the Office of CRCL. Pursuant to exemptions (k)(1), (k)(2) and (k)(5) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3);

(d); (e)(1); (e)(4)(G), (H) and (I) and (f). Exemptions from the particular subsections are justified, on a case by case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of DHS or another agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension, which undermines the entire system.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Access to the records would permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously re-investigated. The information contained in the system may also include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information also could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced, occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective enforcement of federal laws, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (H) and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access provisions of subsection (d).

[71 FR 20523, Apr. 21, 2006]

## PART 7—CLASSIFIED NATIONAL SECURITY INFORMATION

### Sec.

- 7.1 Purpose.
- 7.2 Scope.
- 7.3 Definitions.

### Subpart A—Administration

- 7.10 Authority of the Chief Security Officer, Office of Security.
- 7.11 Components' responsibilities.
- 7.12 Violations of classified information requirements.
- 7.13 Judicial proceedings.

### Subpart B—Classified Information

- 7.20 Classification and declassification authority.
- 7.21 Classification of information, limitations.
- 7.22 Classification pending review.
- 7.23 Emergency release of classified information.
- 7.24 Duration of classification.
- 7.25 Identification and markings.
- 7.26 Derivative classification.
- 7.27 Declassification and downgrading.
- 7.28 Automatic declassification.
- 7.29 Documents of permanent historical value.
- 7.30 Classification challenges.
- 7.31 Mandatory review for declassification requests.

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

SOURCE: 70 FR 61213, Oct. 21, 2005, unless otherwise noted.

#### § 7.1 Purpose.

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

#### § 7.2 Scope.

(a) This part applies to all employees, detailees and non-contractor personnel outside the Executive Branch who are granted access to classified information by the DHS, in accordance