SUPPLEMENT NO. 7 TO PART 748—AUTHORIZATION VALIDATED END-USER (VEU): LIST OF VALIDATED END-USERS, RESPECTIVE ITEMS ELIGIBLE FOR EXPORT, REEXPORT AND TRANSFER, AND ELIGIBLE DESTINATIONS—Continued

Country	Validated end-user	Eligible items (by ECCN)	Eligible destination	**Federal Register** citation
		This item is authorized for those Applied Materials Destination Identified by three asterisks (***): 3E001 (limited to ''technology'' according to the General Technology Note for the ''development'' or ''production'' of items controlled by ECCN 3B001).	*** Applied Materials (China), Inc.—Headquarters, 1388 Zhangdong Road, Bldg. 22, Zhangjiang Hi-Tech Park, Pudong, Shanghai, 201203, China.	
*	*	*	*	*	*	*

Dated: October 21, 2015.

Matthew S. Borman,

Deputy Assistant Secretary for Export Administration.

[FR Doc. 2015–27442 Filed 10–27–15; 8:45 am]

BILLING CODE 3510–33–P

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 197

[Docket ID: DoD–2013–OS–0108]

RIN 0790–AJ07

Historical Research in the Files of the Office of the Secretary of Defense (OSD)

AGENCY: Department of Defense.

ACTION: Final rule.

SUMMARY: This final rule updates and clarifies procedures regarding the review and accessibility to records and information in the custody of the Secretary of Defense and the OSD Components. The purpose of this rule is to provide such guidance to former Cabinet level officials and former Presidential appointees (FPAs), including their personnel, aides, and official researchers.

DATES: This rule is effective November 27, 2015.

FOR FURTHER INFORMATION CONTACT: Mr. Ronald R. McCully, 571–372–0473.

SUPPLEMENTARY INFORMATION:

I. Executive Summary

A. Purpose of the Regulatory Action

a. The Office of the Secretary of Defense (OSD) is issuing a final rule that would update Part 197.5 of Title 32, Code of Federal Regulations. This final rule updates and clarifies procedures regarding the review and accessibility to records and information in the custody of the Secretary of Defense and the OSD Components. The purpose of this rule is to provide such guidance to former Cabinet level officials and former Presidential appointees (FPAs), including their personnel, aides, and official researchers.

b. In accordance with Title 5 of the United States Code, ''Government Organization and Employees,'' this rule updates procedures for the programs that permit authorized personnel to perform historical research in records created by or in the custody of Office of the Secretary of Defense and its components consistent with federal regulations.

B. Summary of the Major Provisions of the Regulatory Action In Question

This final rule updates and clarifies procedures regarding the review and accessibility to records and information in the custody of the Secretary of Defense and the OSD Components. The purpose of this rule is to provide such guidance to former Cabinet level officials and former Presidential appointees (FPAs), including their personnel, aides, and official researchers.

1. *Explanation of FOIA Exemptions and Classification Categories*: Explanation of restrictions applicable to the public's request for information within OSD files.

2. *Responsibilities*: Outlines the responsibilities of Director of Administration and Management (D&AM); OSD Records Administrator, and the OSD Components.

3. *Procedures for Historical Researchers Permanently Assigned Within the Executive Branch Working on Official Projects*: Updates and outlines procedures for access to information held within OSD files for historical research.

4. *Procedures for the Department of State (DoS) Foreign Relations of the United States (FRUS) Series*: Updates and outlines for official researchers of the DOS to access information within OSD Files.

5. *Procedures for Historical Researchers Not Permanently Assigned to the Executive Branch*: Updates and outlines procedures for Non DoD and executive branch personnel to access information within OSD files for historical research.

6. *Procedures for Document Review for the FRUS Series*: Updates and outlines procedures for reviewing FRUS information within OSD files for historical research.

7. *Procedures for Copying Documents*: Updates and outlines procedures for copying information within OSD files for historical research.

8. *General Guidelines for Researching OSD Records*: Updates and outlines procedures for researching information within OSD files for historical research.

9. *General Guidelines for Researching OSD Records*: Updates and outlines guidelines applicable to researchers while reviewing OSD files.

C. Costs and Benefits

Annual yearly cost vary and are dependent on the number of researchers requesting access to DoD owned information, the volume of information requiring review and/or declassification and other operational constraints within a given FY.

Cost: Cost estimates use actual data for 2012 per hour. Cost is aggregated based on average rank (military), grade (civilian) and time in service for personnel qualified for oversight of researchers within the Washington-Baltimore-Northern Virginia, DC-MD-VA-WV-PA area.

Military = Rank 05 with 10+ years of time in service

Civilian = Grade GS–13, Step 5+ with minimum 5 years of time in service

Military = $39.77 per hour

Civilian = $48.51 per hour

Benefit: This allows the government to assert positive control over access to classified and unclassified information requested for research purposes. DoD information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the DoD shall be reviewed for clearance prior to release.

II. Public Comments

On Thursday, May 8, 2014 (79 FR 26381–26391), the Department of Defense published a proposed rule requesting public comment. At the end of the 60-day public comment period, 1 comment was received.

Comment: OGIS commends OSD for providing access guidance to former Cabinet-level officials and former Presidential appointees (FPAs), including their personnel, aides, and official researchers, particularly in regard to the nine FOIA exemptions, summarized in the ''Table—Explanation of FOIA Exemptions.''

The Table describes Exemption (b)(4) as protecting ''trade secrets and commercial or financial information obtained from a *private* source which would cause substantial competitive harm to the source if disclosed.'' (Emphasis added) OGIS notes that Exemption 4 applies to material obtained from a variety of sources, both public and private. Such sources may include ''state governments, agencies of foreign governments, and Native American tribes or nations,'' according to the Department of Justice Guide to the Freedom of Information Act, *http://www.justice.gov/oip/foia_guide09/exemption4.pdf#_PAGE1.*

As such, OGIS suggests clarifying by changing ''from a private source'' to ''a non-U.S. Government source.''

Response: OSD concurs and, in consultation with the OSD FOIA Office, we will include in the next revision or update of the regulation.

III. Regulatory Procedures

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

Executive Orders 13563 and 12866 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distribute impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has not been designated a ''significant regulatory action,'' because the rule does not have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities; create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency; materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in these Executive Orders.

Unfunded Mandates Reform Act (Sec. 202, Pub. L. 104–4)

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

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

The Department of Defense certifies that this final rule is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. Therefore, the Regulatory Flexibility Act, as amended, does not require us to prepare a regulatory flexibility analysis.

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

It has been certified that this rule does not impose reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995.

Executive Order 13132, ''Federalism''

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

List of Subjects in 32 CFR Part 197

Historical records, Research.

Accordingly, 32 CFR part 197 is revised to read as follows:

PART 197—HISTORICAL RESEARCH IN THE FILES OF THE OFFICE OF THE SECRETARY OF DEFENSE (OSD)

Sec.

Authority: 5 U.S.C. 301, Executive Order 13526, 5 U.S.C. 552b, and Pub. L. 102–138.

§ 197.1 Purpose.

This part, in accordance with the authority in DoD Directive 5110.4, implements policy and updates procedures for the programs that permit authorized personnel to perform historical research in records created by or in the custody of Office of the Secretary of Defense (OSD) consistent with Executive Order 13526; DoD Manual 5230.30, ''DoD Mandatory Declassification Review (MDR) Program'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/523030m.pdf*); 32 CFR part 286; 32 CFR part 310; DoD Manual 5200.01, ''DoD Information Security Program'' Volumes 1–4 (available at *http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf, http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf, http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf,* and *http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf*); 36 CFR 1230.10 and 36 CFR part 1236; DoD Directive 5230.09, ''Clearance of DoD Information for Public Release'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/523009p.pdf*); and 32 CFR 197.5.

§ 197.2 Applicability.

This part applies to:

(a) The Office of the Secretary of Defense (OSD), the Defense Agencies, and the DoD Field Activities in the National Capital Region that are serviced by Washington Headquarters Services (WHS) (referred to collectively in this part as the ''WHS-Serviced Components'').

(b) All historical researchers as defined in § 197.3.

(c) Cabinet Level Officials, Former Presidential Appointees (FPAs) to include their personnel, aides and researchers, seeking access to records containing information they originated, reviewed, signed, or received while serving in an official capacity.

§ 197.3 Definitions.

The following definitions apply to this part:

Access. The availability of or the permission to consult records, archives, or manuscripts. The ability and opportunity to obtain classified, unclassified, or administratively controlled information or records.

Electronic records. Records stored in a form that only a computer can process and satisfies the definition of a federal record, also referred to as machine-readable records or automatic data processing records (including email).

Historical researchers or requestors. A person approved to conduct research in OSD files for historical information to use in a DoD approved project (*e.g.,* agency historical office projects, books, articles, studies, or reports), regardless of the person's employment status. Excluded are Military personnel assigned to OSD; OSD employees, contractors, and students conducting research in response to academic requirements.

Records (also referred to as federal records or official records). All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the U.S. Government or because of the informational value of data in them.

§ 197.4 Policy.

It is OSD policy that:

(a) Pursuant to Executive Order 13526, anyone requesting access to classified material must possess the requisite security clearance.

(b) Members of the public seeking the declassification of DoD documents under the provisions of section 3.5 of Executive Order 13526 will contact the appropriate OSD Component as listed in DoD Manual 5230.30.

(c) Records and information requested by FPA and approved historical researchers will be accessed at a facility under the control of the National Archives and Records Administration (NARA), NARA's Archives II in College Park, Maryland, a Presidential library, or an appropriate U.S. military facility or a DoD activity in accordance with Vol 3 of DoD Manual 5200.01, ''DoD Information Security Program,'' February 24, 2012, as amended.

(d) Access to records and information will be limited to the specific records within the scope of the proposed research request over which OSD has authority and to any other records for which the written consent of other agencies with authority has been granted in accordance with Vol 3 of DoD Manual 5200.01, ''DoD Information Security Program,'' February 24, 2012, as amended.

(e) Access to unclassified OSD Component records and information will be permitted consistent with the restrictions of the exemptions of 5 U.S.C. 552(b) (also known and referred to in this part as the ''Freedom of Information Act'' (FOIA), 32 CFR part 286, § 197.5 of this part, and consistent with 32 CFR part 310. The procedures for access to classified information will be used if the requested unclassified information is contained in OSD files whose overall markings are classified.

(f) Except as otherwise provided in DoD Manual 5200.01 volume 3, no person may have access to classified information unless that person has been determined to be trustworthy and access is essential to the accomplishment of a lawful and authorized purpose.

(g) Persons outside the Executive Branch who are engaged in approved historical research projects may be granted access to classified information, consistent with the provisions of Executive Order 13526 and DoD Manual 5200.01 volume 1 provided that the OSD official with classification jurisdiction over that information grants access.

(h) Contractors working for Executive Branch agencies may be allowed access to classified OSD Component files provided the contractors meet all the required criteria for such access as an historical researcher including the appropriate level of personnel security clearance set forth in paragraphs (a) and (i) of this section. No copies of OSD records and information may be released directly to the contractors. The Washington Headquarters Services Records and Declassification Division (WHS/RDD) will be responsible for ensuring that the contractor safeguards the documents and the information is only used for the project for which it was requested per section 4.1 of Executive Order 13526, ''Classified National Security Information,'' December 29, 2009.

(i) All DoD-employed requesters, to include DoD contractors, must have critical nuclear weapons design information (CNWDI) to access CNWDI information. All other non DoD and non-Executive Branch personnel must have a Department of Energy-issued ''Q'' clearance to access CNWDI information in accordance with DoD Manual 5220.22, ''National Industrial Security Program Operating Manual (NISPOM),'' February 28, 2006, as amended.

(j) The removal of federal records and information from OSD custody is not authorized; this includes copies and email according to 36 CFR 1230.10. Copies of records and information that are national security classified will remain under the control of the agency.

(k) Access for FPAs is limited to records they originated, reviewed, signed, or received while serving as Presidential appointees, unless there is another basis for providing access in accordance with Vol 3 of DoD Manual 5200.01, ''DoD Information Security Program,'' February 24, 2012, as amended.

(l) Authorization is required from all agencies whose classified information is, or is expected to be, in the requested files prior to granting approval for access. Separate authorizations for access to records and information maintained in OSD Component office files or at the federal records centers will not be required in accordance with Vol 3 of DoD Manual 5200.01, ''DoD Information Security Program,'' February 24, 2012, as amended.

§ 197.5 Responsibilities.

(a) The Director of Administration (DA), Office of the Deputy Chief Management Officer (ODCMO), or designee is the approval authority for access to DoD information in OSD Component files and in files at the National Archives, Presidential libraries, and other similar institutions in accordance with DoD Directive 5110.4 and DoD Manual 5230.30.

(b) *OSD Records Administrator.* Under the authority, direction, and control of the DA, ODCMO, the OSD Records Administrator:

(1) Exercises approval authority for research access to OSD and WHS Serviced Components records, information, and the Historical Research Program.

(2) Maintains records necessary to process and monitor each case.

(3) Obtains all required authorizations.

(4) Obtains, when warranted, the legal opinion of the General Counsel of the

Department of Defense regarding the requested access.

(5) Coordinates, with the originator, on the public release review on documents selected by the researchers for use in unclassified projects in accordance with DoD Directive 5230.09 and DoD Instruction 5230.29, ''Security and Policy Review of DoD Information for Public Release'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/523029p.pdf*).

(6) Coordinates requests with the OSD Historian.

(7) Provides prospective researchers the procedures necessary for requesting access to OSD Component files.

(c) The WHS-serviced Components heads, when requested:

(1) Determine whether access is for a lawful and authorized government purpose or in the interest of national security.

(2) Determine whether the specific records requested are within the scope of the proposed historical research.

(3) Determine the location of the requested records.

(4) Provide a point of contact to the OSD Records Administrator.

§ 197.6 Procedures.

(a) *Procedures for historical researchers permanently assigned within the Executive Branch working on official projects.* (1) In accordance with § 197.5, the WHS-serviced Components heads, when requested, will:

(i) Make a written determination that the requested access is essential to the accomplishment of a lawful and authorized U.S. Government purpose, stating whether the requested records can be made available. If disapproved, cite specific reasons.

(ii) Provide the location of the requested records, including accession and box numbers if the material has been retired to the Washington National Records Center (WNRC).

(iii) Provide a point of contact for liaison with the OSD Records Administrator if any requested records are located in OSD Component working files.

(2) The historical researcher or requestor will:

(i) Submit a request for access to OSD files to: OSD Records Administrator, WHS/Records and Declassification Division, 4800 Mark Center Drive, Suite 02F09–02, Alexandria, VA 22350–3100.

(ii) All requests must be signed by an appropriate official and must contain:

(A) The name(s) of the researcher(s) and any assistant(s), level of security clearance, and the federal agency, institute, or company to which the researcher is assigned.

(B) A statement on the purpose of the project, including whether the final product is to be classified or unclassified.

(C) An explicit description of the information being requested and, if known, the originating office, so that the identification and location of the information may be facilitated.

(D) Appropriate higher authorization of the request.

(E) Ensure researcher's security manager or personnel security office verifies his or her security clearances in writing to the OSD Records Administrator's Security Manager.

(iii) Maintain the file integrity of the records being reviewed, ensuring that no records are removed and that all folders are replaced in the correct box in their proper order.

(iv) Make copies of any documents pertinent to the project, ensuring that staples are carefully removed and that the documents are re-stapled before they are replaced in the folder.

(v) Submit the completed manuscript for review prior to public presentation or publication to: WHS/Chief, Security Review Division, Office of Security Review, 1155 Defense Pentagon, Washington, DC 20301–1155.

(vi) If the requester is an official historian of a federal agency requiring access to DoD records at the National Archives facilities or a Presidential library, the requested must be addressed directly to the pertinent facility with an information copy sent to the OSD Records Administrator. The historian's security clearances must be verified to the National Archives or the Presidential library.

(3) The use of computers, laptops, computer tablets, personal digital assistants, recorders, or similar devices listed in § 197.6(f) is prohibited. Researchers will use letter-sized paper (approximately 8½ by 11 inches), writing on only one side of the page. Each page of notes must pertain to only one document.

(4) The following applies to all notes taken during research:

(i) All notes are considered classified at the level of the document from which they were taken.

(ii) Indicate at the top of each page of notes the document:

(A) Originator.

(B) Date.

(C) Subject (if the subject is classified, indicate the classification).

(D) Folder number or other identification.

(E) Accession number and box number in which the document was found.

(F) Security classification of the document.

(iii) Number each page of notes consecutively.

(iv) Leave the last 1½ inches on the bottom of each page of notes blank for use by the reviewing agencies.

(v) Ensure the notes are legible, in English, and in black ink.

(vi) All notes must be given to the staff at the end of each day. The facility staff will forward the notes to the OSD Records Administrator for an official review and release to the researcher.

(5) The OSD Records Administrator will:

(i) Process all requests from Executive Branch employees requesting access to OSD Component files for official projects.

(ii) Determine which OSD Component originated the requested records and, if necessary, request an access determination from the OSD Component and the location of the requested records, including but not limited to electronic information systems, databases or accession number and box numbers if the hardcopy records have been retired offsite.

(iii) Request authorization for access from other OSD Component as necessary.

(A) Official historians employed by federal agencies may have access to the classified information of any other agency found in DoD files, as long as authorization for access has been obtained from these agencies.

(B) If the requester is not an official historian, authorization for access must be obtained from the Central Intelligence Agency (CIA), National Security Council (NSC), Department of State (DOS), and any other non-DoD agency whose classified information is expected to be found in the files to be accessed.

(iv) Make a written determination as to the researcher's trustworthiness based on the researcher having been issued a security clearance.

(v) Compile all information on the request for access to classified information, to include evidence of an appropriately issued personnel security clearance, and forward the information to the DA, ODCMO; OSD Component or designee, who will make the access determination.

(vi) Notify the researcher of the authorization and conditions for access to the requested records or of the denial of access and the reason(s).

(vii) Ensure that all conditions for access and release of information for use in the project are met.

(viii) Make all necessary arrangements for the researcher to visit the review location and review the requested records.

(ix) Provide all requested records and information under OSD control in electronic formats consistent with 36 CFR part 1236. For all other information, a staff member will be assigned to supervise the researcher's copying of pertinent documents at the assigned facility.

(x) If the records are maintained in the OSD Component's working files, arrange for the material to be converted to electronic format for the researchers to review.

(xi) Notify the National Archives, Presidential library, or military facility of the authorization and access conditions of all researchers approved to research OSD records held in those facilities.

(b) *Procedures for the DOS Foreign Relations of the United States (FRUS) series.* (1) The DOS historians will:

(i) Submit requests for access to OSD files. The request should list the names and security clearances for the historians doing the research and an explicit description, including the accession and box numbers, of the files being requested. Submit request to: OSD Records Administrator, WHS/Records and Declassification Division, 4800 Mark Center Dr, Suite 02F09–02, Alexandria, VA 22380–2100.

(ii) Submit to the OSD Records Administrator requests for access for members of the Advisory Committee on Historical Diplomatic Documentation to documents copied by the DOS historians for the series or the files reviewed to obtain the documents.

(iii) Request that the DOS Diplomatic Security staff verify all security clearances in writing to the OSD Records Administrator's Security Manager.

(iv) Give all document copies to the OSD Records Administrator staff member who is supervising the copying as they are made.

(v) Submit any OSD documents desired for use or pages of the manuscript containing OSD classified information for declassification review prior to publication to the Chief, Security Review Division at: WHS/Chief, Security Review Division, Office of Security Review, 1155 Defense Pentagon, Washington, DC 20301–1155.

(2) The OSD Records Administrator will:

(i) Determine the location of the records being requested by the DOS for the FRUS series according to Title IV of Public Law 102–138, ''The Foreign Relations of the United States Historical Series.''

(ii) Act as a liaison with the CIA, NSC, and any other non-OSD agency for access by DOS historians to records and information and such non-DoD agency classified information expected to be interfiled with the requested OSD records.

(iii) Obtain written verification from the DOS Diplomatic Security staff of all security clearances, including ''Q'' clearances.

(iv) Make all necessary arrangements for the DOS historians to access, review, and copy documents selected for use in their research in accordance with procedures in accordance with § 197.6(a).

(v) Provide a staff member to supervise document copying in accordance with the guidance provided in § 197.6(d) of this part.

(vi) Compile a list of the documents that were copied by the DOS historians.

(vii) Scan and transfer copies to DOS in NARA an approved electronic format.

(viii) Submit to the respective agency a list of CIA and NSC documents copied and released to the DOS historians.

(ix) Process DOS Historian Office requests for members of the Advisory Committee on Historical Diplomatic Documentation with appropriate security clearances to have access to documents copied and used by the DOS historians to compile the FRUS series volumes or to the files that were reviewed to obtain the copied documents. Make all necessary arrangements for the Advisory Committee to review any documents that are at the WNRC.

(c) *Procedures for historical researchers not permanently assigned to the Executive Branch.* (1) The WHS-serviced Components heads, when required, will:

(i) Recommend to the DA, ODCMO, or his or her designee, approval or disapproval of requests to access OSD information. State whether access to, release, and clearance of the requested information is in the interest of national security and whether the information can be made available. If disapproval is recommended, specific reasons should be cited.

(ii) Provide the location of the requested information, including but not limited to the office, component, information system or accession and box numbers for any records that have been retired to the WNRC.

(iii) Provide a point of contact for liaison with the OSD Records Administrator if any requested records are located in OSD Component working files.

(2) The OSD Records Administrator will:

(i) Process all requests from non-Executive Branch researchers for access to OSD or WHS-serviced Components files. Certify via the WHS Security Officer that the requester has the appropriate clearances.

(ii) Determine which OSD Component originated the requested records and, as necessary, obtain written recommendations for the research to review the classified information.

(iii) Obtain prior authorization to review their classified information from the DOS, CIA, NSC, and any other agency whose classified information is expected to be interfiled with OSD records.

(iv) Obtain agreement from the researcher(s) and any assistant(s) that they will comply with conditions governing access to the classified information (see Figure to § 197.6).

Figure to § 197.6. Form Letter – Conditions Governing Access to Official Records for Historical Research Purposes

(LETTERHEAD STATIONERY)

Date:

OSD Records Administrator

WHS/Records and Declassification Division

4800 Mark Center Drive

Suite 02F09-02

Alexandria Va 22350-3100

To Whom It May Concern:

I understand that the information to which I have requested access for historical research purposes may include information concerning the national defense or foreign relations of the United States. Unauthorized disclosure could reasonably be expected to cause damage, serious damage, or exceptionally grave damage to the national security regardless of the classification of that information. If granted access, I therefore agree to the following conditions governing access to OSD files:

1. I will abide by any rules and restrictions issued in your letter of authorization, including those of other agencies whose information is interfiled with that of the OSD.

2. I agree to safeguard the classified information to which I gain possession or knowledge in a manner consistent with Part 4 of Executive Order 13526, "Classified National Security Information," and the applicable provisions of the DoD issuances concerning safeguarding classified information, including DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information."

3. I agree not to reveal to any person or agency any information obtained as a result of this access except as authorized in the terms of your authorization letter or a follow-on letter. I further agree that I will not use the information for purposes other than those set forth in my request for access.

4. I agree to submit my research notes to determine if classified information is contained in them before their removal from the specific area assigned to me for research. I further agree to submit my manuscript for a security review before its publication or presentation. In each of these reviews, I agree to comply with any decision of the reviewing official in the interests of the security of the United States, including the retention or deletion of any classified parts of such notes and manuscript whenever the federal agency concerned deems such retention or deletion necessary.

5. I understand that failure to abide by the conditions in this statement constitutes sufficient cause for canceling my access to OSD information and for denying me any future access and may subject me to criminal provisions of federal law as referred to in paragraph 6.

6. I have been informed that provisions of Title 18 of the United States Code impose criminal penalties, under certain circumstances, for the unauthorized disclosure, loss, copying, or destruction of defense information.

7. Removal Subject to a Nondisclosure Agreement. Cabinet Level officials may remove copies of unclassified information and/or materials not previously released to the public or with clearly identified restrictions upon request of the departing official if he or she signs a non-disclosure agreement. The former official must agree not to release or publish the information, orally or in writings (paper or electronically), without the written approval of the DoD. Upon request by the Cabinet level official, the DoD will perform an official review of the information. The review may result in possible denial or redaction of the information. The Director of Administration and Management will serve as the appellate authority to any denials or redactions that may be contested.

Signature

THIS STATEMENT IS MADE TO THE UNITED STATES GOVERNMENT TO ENABLE IT TO EXERCISE ITS RESPONSIBILITY FOR THE PROTECTION OF INFORMATION AFFECTING THE NATIONAL SECURITY. I UNDERSTAND THAT ANY MATERIAL FALSE STATEMENT THAT I MAKE KNOWINGLY AND WILLFULLY SHALL SUBJECT ME TO THE PENALTIES OF TITLE 18, U.S. CODE, SECTION 1001.

(v) If the requester is an FPA, submit a memorandum after completion of the actions described in this part to WHS, Human Resources Directorate, Security Operations Division, requesting the issuance (including an interim) or

reinstatement of an inactive security clearance for the FPA and any assistant and a copy of any signed form letters. The Security Division will contact the researcher(s) and any assistant(s) to obtain the forms required to reinstate or initiate the personnel security investigation to obtain a security clearance. Upon completion of the adjudication process, notify the OSD Records Administrator in writing of the reinstatement, issuance, or denial of a security clearance.

(vi) Make a written determination as to the researcher's trustworthiness based on his or her having been issued a security clearance.

(vii) Compile all information on the request for access to classified information, to include either evidence of an appropriately issued or reinstated personnel security clearance. Forward the information to the DA, ODCMO or designee, who will make the final determination on the applicant's eligibility for access to classified OSD or WHS-serviced Component files. If the determination is favorable, the DA, ODCMO or designee will then execute an authorization for access, which will be valid for not more than 2 years.

(viii) Notify the researcher of the approval or disapproval of the request. If the request has been approved, the notification will identify the files authorized for review and specify that the authorization:

(A) Is approved for a predetermined time period.

(B) Is limited to the designated files.

(C) Does not include access to records and/or information of other federal agencies, unless such access has been specifically authorized by those agencies.

(ix) Make all necessary arrangements for the researcher to visit the WNRC and review any requested records that have been retired there, to include written authorization, conditions for the access, and a copy of the security clearance verification.

(x) If the requested records are at the WNRC, make all necessary arrangements for the scanning of documents.

(xi) If the requested records are maintained in OSD or WHS-serviced Component working files, make arrangements for the researcher to review the requested information and, if authorized, copy pertinent documents in the OSD or WHS-serviced Component's office. Provide the OSD Component with a copy of the written authorization and conditions under which the access is permitted.

(xii) Compile a list of all the documents requested by the researcher.

(xiii) Coordinate the official review on all notes taken and documents copied by the researcher.

(xiv) If the classified information to be reviewed is on file at the National Archives, a Presidential library, or other facility, notify the pertinent facility in writing of the authorization and conditions for access.

(3) The researcher will:

(i) Submit a request for access to OSD Component files to OSD Records Administrator, WHS/Records and Declassification Division, 4800 Mark Center Drive, Suite 02F09–02, Alexandria VA 22350–3100. The request must contain:

(A) As explicit a description as possible of the information being requested so that identification and location of the information may be facilitated.

(B) A statement as to how the information will be used, including whether the final project is to be classified or unclassified.

(C) A statement as to whether the researcher has a security clearance, including the level of clearance and the name of the issuing agency.

(D) The names of any persons who will be assisting the researcher with the project. If the assistants have security clearances, provide the level of clearance and the name of the issuing agency.

(E) A signed copy of their agreement (see Figure) to safeguard the information and to authorize a review of any notes and manuscript for a determination that they contain no classified information. Each project assistant must also sign a copy of the letter.

(F) The forms necessary to obtain a security clearance, if the requester is an FPA without an active security clearance. Each project assistant without an active security clearance will also need to complete these forms. If the FPA or assistant have current security clearances, their personnel security office must provide verification in writing to the OSD Records Administrator's Security Manager.

(ii) Maintain the integrity of the files being reviewed, ensuring that no records are removed and that all folders are replaced in the correct box in their proper order.

(iii) If copies are authorized, give all copies to the custodian of the files at the end of each day. The custodian will forward the copies of the documents to the OSD Records Administrator for a declassification review and release to the requester.

(A) For records at the WNRC, if authorized, provide the requested information in an electronic format. Review will occur only in the presence of an OSD Records Administrator staff member.

(B) Ensure that all staples are carefully removed and that the documents are re-stapled before the documents are replaced in the folder.

(C) Submit all classified and unclassified notes made from the records to the custodian of the files at the end of each day of research. The custodian will transmit the notes to the OSD Records Administrator for an official review and release to the researcher at the completion of researcher's project.

(D) Submit the final manuscript to the OSD Records Administrator for forwarding to the Chief, Security Review Division, Office of Security Review, for a security review and public release clearance in accordance with DoD Directive 5230.09 and DoD 5220.22–M, ''National Industrial Security Program Operating Manual (NISPOM)'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf*) prior to publication, presentation, or any other public use.

(d) *Procedures for document review for the FRUS series.* (1) When documents are being reviewed, a WHS/RDD staff member must be present at all times.

(2) The records maybe reviewed at a Presidential Library Archives II, College Park Maryland, WNRC, Suitland, Maryland, or an appropriate military facility. All requested information will remain under the control of the WHS/RDD staff until a public release review is completed, and then provided in electronic formats.

(3) If the requested records have been reviewed in accordance with the automatic declassification provisions of Executive Order 13526, any tabs removed during the research and copying must be replaced in accordance with DoD Manual 5200.01 volume 2.

(4) The number of boxes to be reviewed will determine which of the following procedures will apply. The WHS/RDD staff member will make that determination at the time the request is processed. When the historian completes the review of the boxes, he or she must contact the WHS/RDD to establish a final schedule for scanning the documents. To avoid a possible delay, a tentative schedule will be established at the time that the review schedule is set.

(i) For 24 boxes or fewer, review and scanning will take place simultaneously. Estimated time to complete scanning is 7 work days.

(ii) For 25 boxes or more, the historian will review the boxes and mark the

documents that are to be scanned using WHS/RDD authorized reproduction tabs.

(iii) If the review occurs at facilities that OSD does not control ownership of the document, the documents must be given to the WHS/RDD staff member for transmittal for processing.

(5) WHS/RDD will notify the historian when the documents are ready to be picked up. All administrative procedures for classified material transfers will be followed in accordance with DoD Manual 5200.01 volume 1 and DoD 5220.22–M and appropriate receipt for unclassified information will be used.

(e) *Procedures for copying documents.* (1) The records will be reviewed and copied at a Presidential Library, Archives II, College Park Maryland, WNRC, Suitland, Maryland, or an appropriate U.S. military facility.

(2) If the requested records have been reviewed in accordance with the automatic declassification provisions of Executive Order 13526 any tabs removed during the research and copying must be replaced in accordance with DoD Manual 5200.01 volume 2.

(3) The researcher will mark the documents that he or she wants to copy using WHS/RDD authorized reproduction tabs.

(4) Any notes taken during the review process must be given to the WHS/RDD staff member present for transmittal to the WHS/RDD.

(5) All reproduction charges are to the responsibility of the researcher.

(6) All documents requested will be copied to an approved electronic format by WHS/RDD staff after official review.

(i) The researcher will need to bring paper, staples, staple remover, and stapler.

(ii) When the researcher completes the review of the boxes, he or she must contact the WHS/RDD to establish a final schedule for scanning the requested documents.

(iii) When the documents are scanned, the WHS/RDD will notify the researcher.

(iv) All questions pertaining to the review, copying, or transmittal of OSD documents must be addressed to the WHS/RDD staff member.

(f) *General guidelines for researching DoD records.* DoD records and information are unique and often cannot be replaced should they be lost or damaged. In order to protect its collections and archives, the OSD Records Administrator has set rules that researchers must follow.

(1) Researchers will work in room assigned. Researchers are not allowed in restricted areas.

(2) Special care must be taken in handling all records. Records may not be leaned on, written on, folded, traced from, or handled in any way likely to damage them.

(3) Records should be kept in the same order in which they are presented.

(4) Items that may not be brought into these research areas include, but are not limited to:

(i) Briefcases.

(ii) Cases for equipment (laptop computers).

(iii) Computers. This includes laptops, tablet computers, personal digital assistants, smart phones, and other similar devices.

(iv) Cellular phones.

(v) Computer peripherals including handheld document scanners and digital or analog cameras.

(vi) Containers larger than 9.5″ × 6.25″ (*e.g.,* paper bags, boxes, backpacks, shopping bags, and sleeping bags).

(vii) Food, drinks (includes bottled water) and cigarettes, cigars, or pipes.

(viii) Handbags or purses larger than 9.5″ × 6.25″.

(ix) Luggage.

(x) Musical instruments and their cases.

(xi) Newspapers.

(xii) Outerwear (*e.g.,* raincoats and overcoats).

(xiii) Pets (exception for service animals, *i.e.,* any guide dog or signal dog that is trained to provide a service to a person with a disability).

(xiv) Scissors or other cutting implements.

(xv) Televisions and audio or video equipment.

(xvi) Umbrellas.

(5) Eating, drinking, or smoking is prohibited.

Appendix A to Part 197—Explanation of FOIA Exemptions and Classification Categories

(a) *Explanation of FOIA Exemptions and Classification Categories*—(1) *Explanation of FOIA Exemptions.* Exemptions and their explanations are provided in the Table to Appendix A. See chapter III of 32 CFR part 286 for further information.

TABLE TO APPENDIX A—EXPLANATION OF FOIA EXEMPTIONS

Exemption	Explanation
(b)(1)	Applies to records and information currently and properly classified in the interest of national security.
(b)(2)	Applies to records related solely to the internal personnel rules and practices of an agency.
(b)(3)	Applies to records and information protected by another law that specifically exempts the information from public release.
(b)(4)	Applies to records and information on trade secrets and commercial or financial information obtained from a *private* source which would cause substantial competitive harm to the source if disclosed.
(b)(5)	Applies to records and information of internal records that are deliberative in nature and are part of the decision making process that contain opinions and recommendations.
(b)(6)	Applies to records or information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
(b)(7)	Applies to records or information compiled for law enforcement purposes that could: (a) Reasonably be expected to interfere with law enforcement proceedings; (b) deprive a person of a right to a fair trial or impartial adjudication; (c) reasonably be expected to constitute an unwarranted invasion of the personal privacy of others; (d) disclose the identity of a confidential source; (e) disclose investigative techniques and procedures; or (f) reasonably be expected to endanger the life or physical safety of any individual.
(b)(8)	Applies to records and information for the use of any agency responsible for the regulation or supervision of financial institutions.
(b)(9)	Applies to records and information containing geological and geophysical information (including maps) concerning wells.

(2) *Classification Categories.* Information will not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of Executive Order 13526, and it pertains to one or more of the following:

(i) Military plans, weapons systems, or operations;

(ii) Foreign government information;

(iii) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(iv) Foreign relations or foreign activities of the United States, including confidential sources;

(v) Scientific, technological, or economic matters relating to the national security;

(vi) U.S. Government programs for safeguarding nuclear materials or facilities;

(vii) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(viii) The development, production, or use of weapons of mass destruction.

(b) [Reserved]

Dated: October 22, 2015.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2015–27393 Filed 10–27–15; 8:45 am]

BILLING CODE 5001–06–P

LIBRARY OF CONGRESS

Copyright Office

37 CFR Part 201

[Docket No. 2014–07]

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

AGENCY: U.S. Copyright Office, Library of Congress.

ACTION: Final rule.

SUMMARY: In this final rule, the Librarian of Congress adopts exemptions to the provision of the Digital Millennium Copyright Act (''DMCA'') that prohibits circumvention of technological measures that control access to copyrighted works, codified in section 1201(a)(1) of title 17 of the United States Code. As required under the statute, the Register of Copyrights, following a public proceeding, submitted a Recommendation concerning proposed exemptions to the Librarian of Congress. After careful consideration, the Librarian adopts final regulations based upon the Register's Recommendation.

DATES: Effective October 28, 2015.

FOR FURTHER INFORMATION CONTACT: Jacqueline C. Charlesworth, General Counsel and Associate Register of Copyrights, by email at *jcharlesworth@loc.gov* or by telephone at 202–707–8350; Sarang V. Damle, Deputy General Counsel, by email at *sdam@loc.gov* or by telephone at 202–707–8350; or Stephen Ruwe, Assistant General Counsel, by email at *sruwe@loc.gov* or by telephone at 202–707–8350.

SUPPLEMENTARY INFORMATION: The Librarian of Congress, pursuant to section 1201(a)(1) of title 17, United States Code, has determined in this sixth triennial rulemaking proceeding that the prohibition against circumvention of technological measures that effectively control access to copyrighted works shall not apply to persons who engage in noninfringing uses of certain classes of such works. This determination is based upon the Recommendation of the Register of Copyrights, which was transmitted to the Librarian on October 8, 2015.[1]

The below discussion summarizes the rulemaking proceeding and Register's Recommendation, announces the Librarian's determination, and publishes the regulatory text specifying the exempted classes of works. A more complete discussion of the rulemaking process, the evidentiary record, and the Register's analysis can be found in the Register's Recommendation, which is posted at *www.copyright.gov/1201/.*

I. Background

A. Statutory Requirements

Congress enacted the DMCA in 1998 to implement certain provisions of the WIPO Copyright and WIPO Performances and Phonograms Treaties. Among other things, title I of the DMCA, which added a new chapter 12 to title 17 of the U.S. Code, prohibits circumvention of technological measures employed by or on behalf of copyright owners to protect access to their works. In enacting this aspect of the law, Congress observed that technological protection measures (''TPMs'') can ''support new ways of disseminating copyrighted materials to users, and . . . safeguard the availability of legitimate uses of those materials by individuals.'' [2]

Section 1201(a)(1) provides in pertinent part that ''[n]o person shall circumvent a technological measure that effectively controls access to a work protected under [title 17].'' Under the statute, to ''circumvent a technological measure'' means ''to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.'' [3] A technological measure that ''effectively controls access to a work'' is one that ''in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.'' [4]

Section 1201(a)(1), however, also includes what Congress characterized as a ''fail-safe'' mechanism,[5] which requires the Librarian of Congress, following a rulemaking proceeding, to publish any class of copyrighted works as to which the Librarian has determined that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected by the prohibition against circumvention in the succeeding three-year period, thereby exempting that class from the prohibition for that period.[6] The Librarian's determination to grant an exemption is based upon the recommendation of the Register of Copyrights, who conducts the rulemaking proceeding.[7] Congress directed the Register, in turn, to consult with the Assistant Secretary for Communications and Information of the Department of Commerce, who oversees the National Telecommunications and Information Administration (''NTIA''), in the course of formulating her recommendation.[8]

The primary responsibility of the Register and the Librarian in the rulemaking proceeding is to assess whether the implementation of access controls impairs the ability of individuals to make noninfringing uses of copyrighted works within the meaning of section 1201(a)(1). To do this, the Register develops a comprehensive administrative record using information submitted by interested members of the public, and makes recommendations to the Librarian concerning whether exemptions are warranted based on that record.

Under the statutory framework, the Librarian, and thus the Register, must consider ''(i) the availability for use of copyrighted works; (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes; (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

[1] Register of Copyrights, Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights (Oct. 2015) (''Register's Recommendation'').

[2] Staff of H. Comm. on the Judiciary, 105th Cong., Section-by-Section Analysis of H.R. 2281 as Passed by the United States House of Representatives on August 4, 1998, at 6 (Comm. Print 1998).

[3] 17 U.S.C. 1201(a)(3)(A).

[4] 17 U.S.C. 1201(a)(3)(B).

[5] *See* H.R. Rep. No. 105–551, pt. 2, at 36 (1998).

[6] *See* 17 U.S.C. 1201(a)(1).

[7] 17 U.S.C. 1201(a)(1)(C).

[8] *Id.*