



governmentattic.org

"Rummaging in the government's attic"

Description of document:	Department of the Treasury Declassification Guide, 2018
Requested date:	31-March-2020
Release date:	19-May-2020
Posted date:	03-August-2020
Source of document:	FOIA Request FOIA and Transparency Department of the Treasury Washington, DC 20220 Fax: 202-622-3895

The governmentattic.org web site ("the site") is a First Amendment free speech web site, and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

May 19, 2020

RE: 2020-04-001

VIA EMAIL

This is the Department of the Treasury's (Treasury) final response to your Freedom of Information Act (FOIA) request dated March 31, 2020. You requested "a copy of the Department of the Treasury Declassification Guide, which was approved by ISCAP on 12/3/2018 and is listed on page 8 of this document <https://www.archives.gov/files/isoo/notices/notice-2019-01.pdf>."

Your request has been processed under the provisions of the FOIA, 5 U.S.C. § 552. A review was conducted on one responsive document totaling nine pages. A section of one page will be withheld pursuant to Exemption 6 of the FOIA as described below. There are no fees assessed at this time since allowable charges fell below \$25.

FOIA Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right to privacy. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

Since Treasury's partial denial response constitutes an adverse action, you have the right to appeal this determination within 90 days from the date of this letter. By filing an appeal, you preserve your rights under FOIA and give the agency a chance to review and reconsider your request and the agency's decision. Your appeal must be in writing, signed by you or your representative, and should contain the rationale for your appeal. Please also cite the FOIA reference number noted above. Your appeal should be addressed to:

Ryan Law, Deputy Assistant Secretary for Privacy, Transparency and Records
FOIA Appeal
FOIA and Transparency
Privacy, Transparency, and Records
Department of the Treasury

1500 Pennsylvania Ave., N.W.
Washington, D.C. 20220

If you submit your appeal by mail, clearly mark the letter and the envelope with the words "Freedom of Information Act Appeal." Your appeal must be postmarked or electronically transmitted within **90 days** from the date of this letter.

If you would like to discuss this response before filing an appeal to attempt to resolve your dispute without going through the appeals process, you may contact the FOIA Public Liaison for assistance via email at FOIAPL@treasury.gov, or via phone at (202) 622-8098.

A FOIA Public Liaison is a supervisory official to whom FOIA requesters can raise questions or concerns about the agency's FOIA process. FOIA Public Liaisons can explain agency records, suggest agency offices that may have responsive records, provide an estimated date of completion, and discuss how to reformulate and/or reduce the scope of requests in order to minimize fees and expedite processing time.

If you are unable to resolve your FOIA dispute through our FOIA Public Liaison, the Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and federal agencies as a non-exclusive alternative to litigation. If you wish to contact OGIS, you may contact the agency directly at the following address, email, fax or telephone numbers:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road – OGIS
College Park, MD 20740-6001
Email: ogis@nara.gov
Telephone: 202-741-5770
Toll free: 1-877-684-6448
Fax: 202-741-5769

Please note that contacting any agency official (including the FOIA analyst, FOIA Requester Service Center, FOIA Public Liaison) and/or OGIS is not an alternative to filing an administrative appeal and does not stop the 90-day appeal clock.

If additional questions arise concerning this action, please contact Scott Longenhagen at (202) 622-2234; or via email at FOIA@treasury.gov. Please reference 2020-04-001.

Sincerely,



Jacqueline J. Scott
FOIA Analyst, FOIA and Transparency
Privacy, Transparency, and Records

UNCLASSIFIED

**(U) Department of the Treasury Declassification Guide
December 3, 2018**

(U) Users of this Guide should use their professional experience when reviewing classified national security information for declassification and conduct the appropriate research to prevent the continued withholding of information that should be released. This research should take into account information previously officially released by the U.S. Government, including information previously declassified by the Interagency Security Classification Appeals Panel (ISCAP):
<https://www.archives.gov/declassification/iscap/decision-table>

(U) Only information detailed in the specific exemption elements in this Guide are authorized to be exempted from declassification at 25 years or later. All other information should be declassified unless the information may be exempted by another agency, or is Restricted Data or Formerly Restricted Data.

(U) If the information falls into those categories it must be referred for review by those with the authority to make that determination in accordance with section 3.3(d)(3) of Executive Order (E.O.) 13526. Instructions on what information may be referred are contained in this Guide.

(U) Before referring information to another government agency, confirm the agency has not waived their equity and is eligible to exempt information as identified in the most recent Information Security Oversight Office (ISOO) Notice that provides guidance on Agencies eligible to receive referrals, available on www.archives.gov/isoo/notices.

(U) If information is not the equity of another agency, and its release does not cause damage to national security, it should be declassified. Other statutes or restrictions may apply before the information may be publicly released.

(U) Only 25X, 50X1-HUM, and 50X2-WMD exemptions may be applied to records reviewed in anticipation of automatic declassification at 25 years (i.e., in reviews conducted in 2018, for records dating between 1974 and 1998). Other than 50X1-HUM and 50X2-WMD, 50X exemptions may only be applied to records approaching automatic declassification at 50 years (i.e., in reviews conducted in 2018, for records dating between 1949 and 1973).

(U) Records exempted under 25X shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin of the record, unless an approved 50X exemption is applied within 5 years of the automatic declassification date. Records exempted under 50X shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin of the record, unless an approved 75X exemption is later applied within 5 years of the automatic declassification date.

(U) This Guide does not allow the Department of the Treasury to incorporate exemptions into its classification guidance under section 2.2(e) of E.O. 13526.

(U) Point of Contact

(U) All inquiries on this guide should be directed to the Department of the Treasury's Office of Security Programs at OSPInformationSecurity@treasury.gov or (b) (6)

UNCLASSIFIED

(U) Department of Treasury's Exemption Authority

(U) The Department of the Treasury has only been authorized to exempt from automatic declassification the limited number of exemptions detailed in this declassification guide. All of these exemptions follow into the X8 category of information defined in section 3.3(b)(8) of E.O. 13526:

“Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructure related to the national security”

(U) Mandatory Declassification Reviews and Freedom of Information Act Reviews

(U) Mandatory Declassification Reviews (MDR) on records 25 years or older must also be in accordance with this Guide. Freedom of Information Act (FOIA) reviews of records 25 year old or older may apply the FOIA (b)(1) to only information that meets the exemption provisions of this Guide (FOIA exemptions (b)(2) through (b)(9) are in no way governed or addressed by this Guide).

(U) National Declassification Center

(U) In accordance with section 3.7(c)(1) of E.O. 13526, this Guide, or detailed declassification guidance, will be provided to the Director of the National Declassification Center at the National Archives and Records Administration.

(U) Referrals

(U) All referrals to other agencies are to be made in accordance with section 3.3(d)(3) of E.O. 13526. Each of the following conditions must be met: the information must originate with another agency (or affect the interests or activities of that agency with respect to classified information); the information must reasonably be expected to fall into an exemption category; and the agency must be eligible to receive referrals as identified in an ISOO Notice, available on www.archives.gov/isoo/notices.

(U) File Series Exemptions

(U) The Department of the Treasury does not have any approved File Series Exemptions (FSEs). The process for FSE approval is in section 3.3(c) of E.O. 13526.

(U) Compromised Information

(U) This section provides guidance for determining if historical records pertaining to the compromise of classified information should be declassified.

(U) Background on Compromised Information

(U) Compromised information results from the unauthorized disclosure or release of classified information. Compromised information is not automatically declassified because of its unauthorized disclosure (see section 1.1(c) of Executive Order (E.O.) 13526). In addition, as described below, information about compromises and follow-on investigations may be classified if an Original

UNCLASSIFIED

Classification Authority determines it is necessary to limit damage, conceal security system vulnerabilities, and preclude further compromise. In some cases, no attempt is made to retrieve compromised information as such attempts would call attention to the compromise, resulting in greater damage to the national security than if no such efforts were made.

(U) Information released pursuant to an authorized official U.S. Government release is *not* compromised information. When a U.S. Government release occurs, including through any of the following means, a reclassification action following the provisions of section 1.7(c) of E.O. 13526 must be conducted to exempt information.

(U) Official U.S. Government releases include information released in:

- U.S. Government publications;
- U.S. Government websites;
- Testimony before the Congress by U.S. Government officials;
- Testimony in judicial proceedings by U.S. Government officials;
- U.S. Government filings in judicial proceedings;
- Prior authorized declassification actions that have been released to the public; and/or
- Statements by the President, the Vice President, or in official White House releases.

(U) *Classification of Compromised Information*

(U) As noted above, compromised information is not automatically declassified because of its unauthorized disclosure. In addition, the location of information, formal analysis of its disclosure, and the fact that classified information has appeared in identifiable public documents or has been disclosed during specific presentations, are classified at the same level [CONFIDENTIAL (C), SECRET (S), or TOP SECRET (TS)], category, duration, with any access limitations (e.g., Sensitive Compartmented Information (SCI)) as the compromised information itself. U.S. Government analysis of compromised information may also be classified depending on the information in the analysis.

(U) Information about compromises and follow-on investigations are classified to limit damage, conceal security system vulnerabilities, and preclude further compromise. If revealed, such information assists adversaries by: (a) alerting them to the fact of a compromise; (b) providing details that would confirm the value of the compromised information; (c) providing information on vulnerabilities leading to or resulting from the compromise; (d) providing insight into investigative and countermeasure procedures; and/or (e) confirming information that would otherwise remain unclear.

(U) When reviewing information regarding compromises, the information remains classified if (1) the information contained in the documents describing the compromise is sufficient to materially assist an adversary in locating the compromised information, and (2) the additional criteria, described below, is satisfied. Regarding the first requirement, the statement "*The New York Times* in 1965 published classified information" does not provide such material assistance, as the volume of material is too great to reasonably search without additional "keys." Similarly, the fact that an unspecified document on a specified broad subject contained classified information would also not provide material assistance; however, identification of a specific report number, date, author, etc., probably would.

UNCLASSIFIED

(U) Second, compromised information or information about investigations of the compromise can only remain classified if all of the following conditions are met:

- 1) There must be an ISCAP-approved exemption for the information element that was compromised;
- 2) The information must be within the date range approved for that information element;
- 3) The information must not fall into the categories in section 1.7 of E.O. 13526; and
- 4) The reviewer must be able to describe the damage to the national security caused by the disclosure.

(U) Section 1.7(a) of E.O. 13526 states:

In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

- (1) conceal violations of law, inefficiency, or administrative error;
- (2) prevent embarrassment to a person, organization, or agency;
- (3) restrain competition; or
- (4) prevent or delay the release of information that does not require protection in the interest of the national security.

(U) If information falls into one of the categories of section 1.7(a), then the information cannot be classified.

(U) In addition, the information must meet the damage criteria established in section 1.1(a)(4) of E.O. 13526, which provides that information may only be classified if its unauthorized disclosure “reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.” Accordingly, if this damage standard is not met, the information must be declassified. *See also* section 3.1(a) of E.O. 13526 (“information shall be declassified as soon as it no longer meets the standards for classification under this order.”).

(U) Treasury’s Exemption Process

(U) Within the Department of the Treasury only the Bureau of Engraving and Printing (BEP) and the U.S. Mint have the authority to exempt information from automatic declassification at 25 years. If the Department of the Treasury determines that additional Department of the Treasury information needs to be exempted from automatic declassification, then approval must be obtained from the ISCAP. Such requests must be routed through and approved by the Department of the Treasury Office of Security Programs.

(U) Bureau of Engraving and Printing (BEP)

(U) Broad Guidance

(U) This Broad Guidance section is for context purposes only and must not be used as exemption authority. Exemption authority is granted only for the detailed exemption information elements.

UNCLASSIFIED

(U) Beginning in 1990, the U.S. Government overtly added advanced security features to the Nation's paper currency, the first major design changes since 1928. Advanced copying technologies raised incidences of counterfeiting. Ink-jet printers, color copiers, and scanners are just a few tools used by criminals and others with interests inimical to the United States to create counterfeit bills. Sophisticated copiers, printers, electronic digital scanners, color workstations, and computer software, which readily interface with each other, present threats to U.S. currency. Such equipment does not require extensive expertise to operate and is widely accessible through copy centers, corporate offices and home use. It is vital to incorporate advanced security features in U.S. currency to effectively counteract such threats.

(U) Counterfeiting of U.S. currency has been kept at low levels through a combination of improvements in security features, aggressive law enforcement and education efforts to inform the world-wide public about how to verify the authenticity of U.S. currency.

(U) The new colors of money are safer, smarter and more secure. They are safer because they make it more difficult to fake and are easier to verify; smarter because they stay ahead of tech-savvy counterfeiters; and more secure because they protect the integrity of U.S. currency and the good faith and credit of the United States. U.S. currency is the world's most familiar and circulated currency, and serves as the primary monetary instrument in the global economy. BEP and Treasury efforts have been to ensure business and financial communities, foreign government, foreign exchange companies, law-enforcement groups, banking officials, and other world-wide cash handlers are secure in their reliance on the integrity of U.S. currency. The loss of acceptance and trust in the validity of U.S. currency has the potential for serious disruption of the U.S. and international banking systems, thereby having a direct bearing on national security.

(U) In keeping with the strategy of maintaining the security of U.S. currency by enhancing the designs periodically, a new series of U.S. currency began to be issued while preserving the distinct size, appearance and "feel" of traditional U.S. currency. This process began with the \$20 note placed in circulation in 2003, followed by the \$50 note issued in 2004, the \$10 note in 2006, the \$5 note in 2007, and a \$100 note in 2013.

(U) U.S. currency circulates world-wide and each newly designed note goes into circulation as domestic and international banks place orders for new currency via the Federal Reserve. Banknote equipment manufacturers are continually updating cash-handling machines to accept new notes. New designs are issued as part of an ongoing overt effort to stay ahead of counterfeiting, to protect the economy, and the hard-earned money of American taxpayers and other users of U.S. currency.

(U) A taggant is also a chemical or physical marker added to materials to allow various forms of testing.

(U) Covert Program Background

(U) Since 1986, BEP has developed and relied on covert authentication systems and forensic features to provide effective means to authenticate U.S. currency. Covert authentication systems provide the Federal Reserve a last line of defense in protecting the monetary system from counterfeiting. These systems also allow the Federal Reserve to detect and remove counterfeit banknotes from circulation. These systems consist of unique materials in the banknotes, quality

UNCLASSIFIED

assurance equipment used to verify at BEP that the notes meet the requirements of the Federal Reserve, and authentication equipment on Federal Reserve currency processors to verify the authenticity of the banknotes. Information that defines the material and the criteria that must be satisfied for authentication to occur are classified at the Secret and Confidential levels. There are multiple covert authentication systems deployed, available for deployment, and under development.

(U) Forensic features are materials that have unique characteristics that are detectable in the laboratory. The U.S. Secret Service utilizes the materials for laboratory authentication of U.S. banknote paper. Some of the forensic features used to detect the unique characteristics are classified at the Secret and Confidential levels.

(U) *Relationship to BEP*

(U) Applicable BEP records are an extremely limited volume of documents critical to continued protection of the integrity of test elements, documents and algorithms associated with the Bureau's covert counterfeit deterrent system program. The documentation is maintained under security controls managed by the BEP. Federal Reserve and Treasury officials have been briefed on the covert program to safeguard U.S. currency. These few documents represent a minute portion of total classified documents that have been examined since the advent of the automatic declassification process.

(U) In conjunction with the BEP, the Department of the Treasury will vigorously review classified material within five years of the automatic declassification at 25 years, as required under Sections 3.3(a) and (b) of the Order. Each review will determine the continued need to exempt these documents from automatic declassification. It is fully understood that failure to review the documents by the prescribed timeframes will result in automatic declassification.

(U) Description: Documents are in hard copy, in textual and electronic format, and pertain to the BEP covert authentication systems and forensic features. Documents are classified as either Secret or Confidential.

(U) Volume: There are approximately 50 documents that have currently been exempted from automatic declassification.

(U) Date Span: Relevant BEP records are from 1986 to the present. Information may only be exempted using the appropriate date determined exemption within 5 years of the documents' current automatic declassification date.

(U) Explanation of why information should be exempt from automatic declassification and remain classified: If information regarding the authentication systems and the forensic features of U.S. currency were subject to automatic declassification, it would cause damage or serious damage to the national security by revealing current vulnerabilities of systems and projects classified in accordance with section 3.3(b)(8) of the Order.

UNCLASSIFIED

(U) Specific Exemptions

(U) Specific information that are not obsolete or superseded by newer technologies that reveals how the following are used to protect currency from counterfeiting. Exempt when covered by the relevant BEP SCG listed on the right, have not been previously declassified, and do not meet the declassification criteria listed below:

Item #	(U) Information To Be Exempted	Exemption	Relevant BEP SCG #
1	(U) Authentication Wavelengths (Universal Currency Authentication System (UCAS)); Authentication Criteria inclusive of illumination design (UCAS2); Spectral information used to detect and/or quantify taggant (Quality Evaluation Detector (QED) or its future replacement (QED2 or equivalent), and Third Party Inspection System (TPIS), Portable Taggant Detector (PTD))	25X8	1
2	(U) Authentication Criteria	25X8	1
3	(U) Chemical Name(s) when associated with Taggant(s)	25X8	1
4	(U) Chemical Formula(s) when associated with Taggant(s)	25X8	1
5	(U) Chemical Structure(s) when associated with Taggant(s)	25X8	1
6	(U) Taggant(s) Concentration	25X8	1
7	(U) Computer Source Code	25X8	1
8	(U) Adversarial Analysis	25X8	1
9	(U) Taggant(s) Vulnerabilities	25X8	1
10	(U) Material Name(s), chemical formula(s), Structure(s) when associated with the system	25X8	2
11	(U) Material detection technologies when associated with system	25X8	2
12	(U) Authentication technologies and criteria	25X8	2
13	(U) System weaknesses and vulnerabilities	25X8	2
14	(U) Inspection and authentication technology requirements	25X8	2
15	(U) Inspections and authentication criteria	25X8	2
16	(U) Chemical name(s) when associated with system	25X8	2
17	(U) Chemical formula(s) when associated with system	25X8	2
18	(U) Chemical structure when associated with system	25X8	2
19	(U) Material(s) Concentration	25X8	2
20	(U) Computer Source Code	25X8	2
21	(U) Adversarial Analysis	25X8	2
22	(U) Material(s) Vulnerabilities	25X8	2
23	(U) Manufacturing methods	25X8	3
24	(U) New fiber research	25X8	3
25	(U) Manufacturing methodology	25X8	3
26	(U) Inspection and Authentication Wavelengths	25X8	4
27	(U) Inspection and Authentication Criteria	25X8	4
28	(U) Chemical Name(s) when Associated with Taggant(s)	25X8	4
29	(U) Chemical Formula(s) when associated with Taggant(s)	25X8	4
30	(U) Chemical Structure(s) when associated with Taggant(s)	25X8	4
31	(U) Taggant(s) Concentration	25X8	4

UNCLASSIFIED

32	(U) Inspection and Authentication Wavelengths	25X8	4
33	(U) Inspection and Authentication Criteria	25X8	4
34	(U) Adversarial Analysis	25X8	4
35	(U) Taggant(s) Vulnerabilities	25X8	4

(U) Declassify

- Declassify when each covert techniques is obsolete or superseded by newer technologies or when the vast regimen of U.S. currency in circulation may no longer be validated by the existing counterfeit deterrent systems and techniques employed by the BEP and the Federal Reserve System.
- Declassify all BEP information prior to 1986.

(U) U.S. Mint

(U) Broad Guidance

(U) This Broad Guidance section is for context purposes only and must not be used as exemption authority. Exemption authority is granted only for the detailed exemption information elements.

(U) Fort Knox, Bullion Depository, 1937 and 1998. This includes approximately 550 detailed blueprints and diagrams showing internal configuration of the Fort Knox Bullion Depository in Kentucky, a secure facility. Fort Knox is a well-known landmark that is referenced in factual and fictitious accounts, and more than any other institution, it symbolizes the economic strength and power of the United States. The Fort Knox facility is also internationally recognized as a benchmark for security.

(U) The Depository offers a tempting target for possible aggression for reasons other than simply theft of gold. It's an attractive target for possible terrorists with political or other interests inimical to the United States. To allow a penetration of the Depository would undoubtedly have world-wide impact and reflect negatively on the country's ability to defend one of its most vital assets. Release of the approximately 550 blueprints/diagrams/plans would reveal the layout and physical makeup of the Fort Knox Bullion Depository and compromise security at the facility.

(U) With respect to current national security emergency preparedness plans, the safeguarding of gold and silver bullion is an economic matter upon which rests the financial stability of the U.S. Government. The gold located at the Depository plays a key role in the nation's defense strategies and under current emergency preparedness plans, gold would be an essential factor in economic stabilization in the event of a nuclear catastrophe and concomitant recovery efforts.

(U) Release of information concerning Fort Knox's structure and contents could jeopardize national security. Without the appropriate exemption, the blueprints and diagrams risk becoming public information and compromising security. Such information should remain classified as long as the Fort Knox Bullion Depository continues to be relied upon to store the nation's gold and silver under section 3.3(b)(8).

(U) In addition, a Security Site survey was conducted in 1985 by the U.S. Secret Service and again in

UNCLASSIFIED

1995 by the combined efforts of ATF, U.S. Marshals Service, FBI and U.S. Mint Police; an analysis of stored materials was conducted by the Mint's special response team, responsible for responding to a hostile takeover of the facility and subsequent removal of intruders. This review reiterated existing security concerns for safeguarding the Fort Knox Bullion Depository.

(U) Description: Documents are in hard copy, paper, blueprint/diagram, text, and electronic formats. Materials are classified either Secret or Confidential.

(U) Volume: Records over 50 years old consist of approximately 400 detailed prints/drawings of the Fort Knox Bullion Depository. Records greater than 25 years old but less than 50 years old consist of approximately 150 detailed prints/drawings of the Fort Knox Bullion Depository. The more recent records volume is approximately 550 documents.

(U) Date Span: Relevant U.S. Mint records are from 1937 to the present. Information may only be exempted using the appropriate date determined exemption within 5 years of the documents current automatic declassification date.

(U) Explanation of why information should be exempt from automatic declassification and remain classified: If information regarding the Fort Knox Bullion Depository were subject to automatic declassification, it would cause damage or serious damage to the national security by revealing current vulnerabilities of systems, installations, and infrastructure that should remain classified in accordance with section 3.3(b)(8) and 3.3(h)(2) and (3) of the Order.

(U) Specific Exemptions

(U) Exempt when they would reveal vulnerabilities to the Fort Knox Bullion Depository, have not been previously declassified, and do not meet the declassification criteria listed below:

Item #	(U) Information To Be Exempted	Exemption	Comments
1	(U) Information describing the security controls used by the U.S. Mint at the Fort Knox Bullion Depository in Kentucky that provides blueprints and diagrams of security features	25X8	Re-review when records are 45-50 years old
2	(U) Detailed blueprints and diagrams showing internal configuration of the Fort Knox Bullion Depository in Kentucky	50X8	Re-review when records are 70-75 years old
3	(U) Detailed blueprints and diagrams showing internal configuration of the Fort Knox Bullion Depository in Kentucky	75X8	Re-review every 5 years to determine if they can be declassified

(U) Declassify

- Declassify when obsolete or superseded by new protections.