(b) *Contents of request.* A request to amend a record in a CIGIE system of records must include:

(1) The name of the system of records and a brief description of the record proposed for amendment. In the event the request to amend the record is the result of the requester having gained access to the record in accordance with the provisions concerning access to records as set forth in subpart B of this part, copies of previous correspondence between the requester and CIGIE will serve in lieu of a separate description of the record.

(2) The exact portion of the record the requester seeks to have amended should be indicated clearly. If possible, proposed alternative language should be set forth, or, at a minimum, the reasons why the requester believes the record is not accurate, relevant, timely, or complete should be set forth with enough particularity to permit CIGIE to not only to understand the requester's basis for the request, but also to make an appropriate amendment to the record.

(c) *Burden of proof.* The requester has the burden of proof when seeking the amendment of a record. The requester must furnish sufficient facts to persuade the appropriate system manager of the inaccuracy, irrelevance, untimeliness, or incompleteness of the record.

(d) *Identification requirement.* When the requester's identity has been previously verified pursuant to § 9801.201, further verification of identity is not required as long as the communication does not suggest a need for verification. If the requester's identity has not been previously verified, the appropriate system manager may require identification validation as described in § 9801.201.

§ 9801.302 Response to requests.

(a) *Time limit for acknowledging a request for amendment.* To the extent possible, CIGIE will acknowledge receipt of a request to amend a record or records within 10 working days.

(b) *Determination on an amendment request.* The decision of CIGIE in response to a request for amendment of a record in a system of records may grant in whole or deny any part of the request to amend the record.

(1) If CIGIE grants the request, the appropriate system manager will amend the record(s) and provide a copy of the amended record(s) to the requester. To the extent an accounting of disclosure has been maintained, the system manager shall advise all previous recipients of the record that an amendment has been made and give the substance of the amendment. Where practicable, the system manager shall send a copy of the amended record to previous recipients.

(2) If CIGIE denies the request in whole or in part, the reasons for the denial will be stated in the response letter. In addition, the response letter will state:

(i) The name and address of the official with whom an appeal of the denial may be lodged; and

(ii) A description of any other procedures which may be required of the requester in order to process the appeal.

§ 9801.303 Appeal from adverse determination on amendment.

(a) *How addressed.* A requester may submit a written appeal of the decision by CIGIE to deny an initial request to amend a record in a CIGIE system of records to the Chairperson, Council of the Inspectors General on Integrity and Efficiency, 1717 H Street NW., Suite 825, Washington, DC 20006. The words ''Privacy Act Appeal'' should be included on the envelope and at the top of the letter of appeal.

(b) *Deadline and content.* The appeal must be received by CIGIE within 60 days of the date of the letter denying the request and should contain a brief description of the record(s) involved or copies of the correspondence from CIGIE and the reasons why the requester believes that the disputed information should be amended.

§ 9801.304 Response to appeal of adverse determination on amendment; disagreement statements.

(a) *Response timing.* The Chairperson should make a final determination in writing not later than 30 days from the date the appeal was received. The 30-day period may be extended for good cause. Notice of the extension and the reasons therefor will be sent to the requester within the 30-day period.

(b) *Amendment granted.* If the Chairperson determines that the record(s) should be amended in accordance with the requester's request, the Chairperson will take the necessary steps to advise the requester and to direct the appropriate system manager:

(1) To amend the record(s); and

(2) To notify previous recipients of the record(s) for which there is an accounting of disclosure that the record(s) have been amended.

(c) *Denial affirmed.* If the appeal decision does not grant in full the request for amendment, the decision letter will notify the requester that the requester may:

(1) Obtain judicial review of the decision in accordance with the terms of the Privacy Act at 5 U.S.C. 552a(g); and

(2) File a statement setting forth their reasons for disagreeing with the decision.

(d) *Requester's disagreement statement.* A requester's disagreement statement must be concise. CIGIE has the authority to determine the ''conciseness'' of the statement, taking into account the scope of the disagreement and the complexity of the issues.

(e) *Provision of requester's disagreement statement.* In any disclosure of information about which an individual has filed a proper statement of disagreement, CIGIE will clearly note any disputed portion(s) of the record(s) and will provide a copy of the statement to persons or other agencies to whom the disputed record or records has been disclosed and for whom an accounting of disclosure has been maintained. A concise statement of the reasons for not making the amendments requested may also be provided.

§ 9801.305 Assistance in preparing request to amend a record or to appeal an initial adverse determination.

Requesters may seek assistance in preparing a request to amend a record or an appeal of an initial adverse determination, or to learn further of the provisions for judicial review, by contacting CIGIE's Privacy Officer by email at *privacy@cigie.gov* or by mail at Privacy Officer, Council of the Inspectors General on Integrity and Efficiency, 1717 H Street NW., Suite 825, Washington, DC 20006.

Dated: August 31, 2016.

Michael E. Horowitz,

Chairperson of the Council of the Inspectors General on Integrity and Efficiency.

[FR Doc. 2016–21473 Filed 9–6–16; 8:45 am]

BILLING CODE 6820–C9–P

FEDERAL TRADE COMMISSION

16 CFR Part 314

RIN 3084–AB35

Standards for Safeguarding Customer Information

AGENCY: Federal Trade Commission.

ACTION: Request for public comment.

SUMMARY: The Federal Trade Commission (''FTC'' or ''Commission'') requests public comment on its Standards for Safeguarding Customer Information (''Safeguards Rule'' or ''Rule''). The Commission is soliciting comment as part of the FTC's systematic review of all current Commission regulations and guides.

DATES: Comments must be received on or before November 7, 2016.

ADDRESSES: Interested parties may file a comment online or on paper by following the Instructions for Submitting Comments part of the **SUPPLEMENTARY INFORMATION** section below. Write ''Safeguards Rule, 16 CFR 314, Project No. P145407,'' on your comment and file your comment online at *https://ftcpublic.commentworks.com/ftc/safeguardsrulenprm* by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW., Suite CC–5610 (Annex B), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW., 5th Floor, Suite 5610 (Annex B), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: David Lincicum or Katherine McCarron, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW., Washington, DC 20580, (202) 326–2773 or (202) 326–2333.

SUPPLEMENTARY INFORMATION:

I. Background

The Gramm-Leach-Bliley Act (''G-L-B Act'' or ''Act'') was enacted in 1999 to reform and modernize the banking industry by eliminating existing barriers between banking and commerce. The Act permits banks to engage in a broad range of activities, including insurance and securities brokering, with new affiliated entities. Subtitle A of Title V of the Act, captioned ''Disclosure of Nonpublic Personal Information,'' limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties, and requires a financial institution to disclose certain information sharing practices. In 2000, the Commission issued a final rule that implemented Subtitle A as it relates to these requirements (hereinafter ''Privacy Rule'').

Subtitle A of Title V also required the Commission and other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information. *See* 15 U.S.C. secs. 6801(b), 6805(b)(2).

Pursuant to the Act's directive, the Commission promulgated the Safeguards Rule in 2002. The Safeguards Rule applies to all ''financial institutions'' over which the Commission has jurisdiction. The Safeguards Rule uses the definition of ''financial institution'' from the Privacy Rule.[1] The Privacy Rule defines ''financial institution'' as ''any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution significantly engaged in financial activities is a financial institution.'' [2] The term ''financial activities'' includes not only a number of traditional financial activities specified in 12 U.S.C. 1843(k), but also those activities found by the Federal Reserve Board (''the Fed'') to be closely related to banking by regulation ''in effect on the date of the enactment'' of the G-L-B Act.[3]

When promulgating the Privacy Rule, the Commission determined to include as ''financial activities'' only those activities that the Fed found to be ''financial in nature,'' and not to include those activities that the Fed found to be ''incidental'' or ''complementary'' to financial activities.[4] Other agencies included ''incidental'' activities when promulgating their rules. In addition, the Commission decided that activities that were determined to be financial in nature after the enactment of the G-L-B Act would not be automatically included in its Privacy Rule; rather, the Commission would have to take additional action to include them. The effect of these two decisions was to limit the activities covered by the Commission's rules to those set out in 12 CFR 225.28 as it existed in 1999. As indicated below, the Commission seeks comment on whether the Safeguards Rule should be amended to include either (1) ''incidental'' activities, or (2) activities determined after 1999 to be financial in nature or ''incidental'' to financial activities.

The Safeguards Rule applies to the handling of ''customer information'' by financial institutions. ''Customer information'' is defined as ''any record containing nonpublic personal information . . . about a customer of a financial institution, whether in paper, electronic, or other form'' that is ''handled or maintained by or on behalf of'' a financial institution or its affiliates.[5] The Rule does not apply to all *consumer* information handled by a financial institution; it applies only to the information of *customers,* which are consumers that have a continuing relationship with a financial institution that provides one or more financial products or services to be used primarily for personal, family, or household purposes.[6] The Rule is not limited to protecting a financial institution's own customers, but also applies to all customer information in the financial institution's possession, including information about the customers of other financial institutions.[7]

The Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive information security program.[8] An information security program consists of the administrative, technical, or physical safeguards the financial institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or

[1] 16 CFR 314.2(a) (terms in the Safeguards Rule have the same meanings as set forth in the Commission's Privacy Rule). Under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Pub. L. 111–203, 124 Stat. 1376 (2010)), the majority of the Commission's rulemaking authority for the Privacy Rule was transferred to the Consumer Financial Protection Bureau (CFPB), with the exception of rulemaking authority pertaining to certain motor vehicle dealers (15 U.S.C. 6804(a)(1)(C)). Accordingly, the Commission's Privacy Rule applies only to certain motor vehicle dealers, while the CFPB's Privacy Rule (12 CFR part 1016) applies to all other entities under the Commission's jurisdiction as well as other financial institutions for which the CFPB has rulemaking authority. The FTC continues to enforce the CFPB Privacy Rule with respect to all entities within the FTC's jurisdiction. Under the Dodd-Frank Act, the Commission retained rulemaking authority for the Safeguards Rule (15 U.S.C. 6804(a)(1)(A)). Thus, for purposes of the Safeguards Rule, the definition of ''financial institution'' in the Commission's Privacy Rule applies to all entities within the Commission's jurisdiction. Other agencies also continue to have rules or guidelines implementing the G-L-B safeguards requirements for entities within their jurisdiction. *See* 12 CFR part 30, app. B (Office of the Comptroller of the Currency); 12 CFR part 208, app. D–2 and 12 CFR part 225, app. F (Board of Governors of the Federal Reserve System); 12 CFR part 364, app. B (Federal Deposit Insurance Corporation); 12 CFR part 748, app. A (National Credit Union Administration); 17 CFR 248.30 (Securities and Exchange Commission).

[2] 16 CFR 313.3(k)(1) (definition of ''financial institution'' in the Privacy Rule).

[3] 65 FR 33,646, 33,647 (May 24, 2000) (discussing scope of Privacy Rule); *see also id.* at 33,654–55 (discussing definition of ''financial institution'').

[4] *Id.* at 33,654.

[5] 16 CFR 314.2(b). ''Nonpublic personal information'' is defined as personally identifiable financial information and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available. 16 CFR 313.3(n)(1). The Safeguards Rule uses the definition of ''nonpublic personal information'' from the Privacy Rule. 16 CFR

[6] 16 CFR 313.3(h), (i). The Safeguards Rule uses the definitions of ''customer'' and ''customer relationship'' from the Privacy Rule. 16 CFR 314.2(a).

[7] 16 CFR 314.1(b).

[8] 16 CFR 314.3(a).

otherwise handle customer information.[9] The information security program must be written in one or more readily accessible parts and contain administrative, technical, and physical safeguards.[10] The safeguards must be appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.[11] The safeguards must also be reasonably designed to insure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[12]

In order to develop, implement, and maintain its information security program, a financial institution must identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, including in the areas of: (1) Employee training and management; (2) information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and (3) detecting, preventing, and responding to attacks, intrusions, or other systems failures.[13] The financial institution must then design and implement information safeguards to control the risks identified through the risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.[14] The financial institution is also required to evaluate and adjust its information security program in light of the results of this testing and monitoring, as well as any material changes in its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on its information security program.[15] The financial institution must also designate an employee or employees to coordinate the information security program.[16]

The Safeguards Rule also requires financial institutions to take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information and require those service providers by contract to implement and maintain such safeguards.[17]

The Safeguards Rule became effective on May 23, 2003.

II. Regulatory Review of the Safeguards Rule

The Commission periodically reviews all of its rules and guides. These reviews seek information about the costs and benefits of the agency's rules and guides, and their regulatory and economic impact. The information obtained assists the Commission in identifying those rules and guides that warrant modification or rescission. Therefore, the Commission solicits comments on, among other things, the economic impact and benefits of the Rule; possible conflict between the Rule and state, local, or other federal laws or regulations; and the effect on the Rule of any technological, economic, or other industry changes.

III. Issues for Comment

The Commission requests written comment on any or all of the following questions. These questions are designed to assist the public and should not be construed as a limitation on the issues about which public comment may be submitted. The Commission requests that responses to its questions be as specific as possible, including a reference to the question being answered, and refer to empirical data or other evidence upon which the comment is based whenever available and appropriate. Please also provide evidence of the prevalence of any unfair acts or practices that any proposed modification would address.

A. General Issues

1. Is there a continuing need for specific provisions of the Rule? Why or why not?

2. What benefits has the Rule provided to consumers? What evidence supports the asserted benefits?

3. What modifications, if any, should be made to the Rule to increase its benefits to consumers?

a. What evidence supports the proposed modifications?

b. How would these modifications affect the costs the Rule imposes on businesses, including small businesses?

4. What significant costs, if any, has the Rule imposed on consumers? What evidence supports the asserted costs?

5. What modifications, if any, should be made to the Rule to reduce any costs imposed on consumers?

a. What evidence supports the proposed modifications?

b. How would these modifications affect the benefits provided by the Rule?

6. What benefits, if any, has the Rule provided to businesses, including small businesses? What evidence supports the asserted benefits?

7. What modifications, if any, should be made to the Rule to increase its benefits to businesses, including small businesses?

a. What evidence supports the proposed modifications?

b. How would these modifications affect the costs the Rule imposes on businesses, including small businesses?

c. How would these modifications affect the benefits to consumers?

8. What significant costs, if any, including costs of compliance, has the Rule imposed on businesses, including small businesses? What evidence supports the asserted costs?

9. What modifications, if any, should be made to the Rule to reduce the costs imposed on businesses, including small businesses?

a. What evidence supports the proposed modifications?

b. How would these modifications affect the benefits provided by the Rule?

10. What evidence is available concerning the degree of industry compliance with the Rule?

11. What modifications, if any, should be made to the Rule to account for changes in relevant technology or economic conditions? What evidence supports the proposed modifications?

12. Does the Rule overlap or conflict with other federal, state, or local laws or regulations? If so, how?

a. What evidence supports the asserted conflicts?

b. With reference to the asserted conflicts, should the Rule be modified? If so, why, and how? If not, why not?

B. Specific Issues

1. Should the elements of an information security program include a response plan in the event of a breach that affects the security, integrity, or confidentiality of customer information? Why or why not? If so, what should such a plan contain?

a. What evidence supports such a modification?

b. How would this modification affect the costs the Rule imposes on businesses, including small businesses?

c. How would this modification affect the benefits to businesses?

d. How would this modification affect the costs the Rule imposes on consumers?

[9] 16 CFR 314.2(c).

[10] 16 CFR 314.3(a).

[11] *Id.*

[12] 16 CFR 314.3(a), (b).

[13] 16 CFR 314.4(b).

[14] 16 CFR 314.4(c).

[15] 16 CFR 314.4(e).

[16] 16 CFR 314.4(a).

[17] 16 CFR 314.4(d).

e. How would this modification affect the benefits to consumers?

2. Should the Rule be modified to include more specific and prescriptive requirements for information security plans? Why or why not? If so, what requirements should be included and what sources should they be drawn from?

a. What evidence supports such a modification?

b. How would this modification affect the costs the Rule imposes on businesses, including small businesses?

c. How would this modification affect the benefits to businesses?

d. How would this modification affect the costs the Rule imposes on consumers?

e. How would this modification affect the benefits to consumers?

3. Should the Rule be modified to reference or incorporate any other information security standards or frameworks, such as the National Institute of Standards and Technology's Cybersecurity Framework or the Payment Card Industry Data Security Standards? If so, which standards should be incorporated or referenced and how should they by referenced or incorporated by the Rule?

a. What evidence supports such a modification?

b. How would this modification affect the costs the Rule imposes on businesses, including small businesses?

c. How would this modification affect the benefits to businesses?

d. How would this modification affect the costs the Rule imposes on consumers?

e. How would this modification affect the benefits to consumers?

4. For the purpose of clarity, should the Rule be modified to include its own definitions of terms, such as ''financial institution'', rather than incorporating the definitions found in the Privacy Rule?

a. What evidence supports such a modification?

b. How would this modification affect the costs the Rule imposes on businesses, including small businesses?

c. How would this modification affect the benefits to businesses?

d. How would this modification affect the costs the Rule imposes on consumers?

e. How would this modification affect the benefits to consumers?

5. The current Safeguards Rule incorporates the Privacy Rule's definition of ''financial institutions'' as entities that are significantly engaged in financial activities, including activities found to be closely related to banking by regulation or order in effect at the time of enactment of the G-L-B Act. Should the Safeguards Rule's definition of ''financial institution'' be modified to also include entities that are significantly engaged in activities that the Federal Reserve Board has found to be incidental to financial activities? Should it also include activities that have been found to be closely related to banking or incidental to financial activities by regulation or order in effect *after* the enactment of the G-L-B Act? [18] If so, should all such activities be included in the modified definition? What evidence supports such a modification?

a. How would this modification affect the costs the Rule imposes on businesses, including small businesses?

b. How would this modification affect the benefits to businesses?

c. How would this modification affect the costs the Rule imposes on consumers?

d. How would this modification affect the benefits to consumers?

IV. Instructions for Submitting Comments

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before November 7, 2016. Write ''Safeguards Rule, 16 CFR 314, Matter No. P145407'' on the comment. Your comment, including your name and your state, will be placed on the public record of this proceeding, including, to the extent practicable, on the public Commission Web site, at *https://www.ftc.gov/policy/public-comments.* As a matter of discretion, the Commission tries to remove individuals' home contact information from comments before placing them on the Commission Web site. Because your comment will be made public, you are solely responsible for making sure that your comment does not include any sensitive personal information, such as a Social Security number, date of birth, driver's license number or other state identification number or foreign country equivalent, passport number, financial account number, or payment card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information.

In addition, do not include any ''[t]rade secret or any commercial or financial information which is . . . privileged or confidential,'' as discussed in Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2). In particular, do not include competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

If you want the Commission to give your comment confidential treatment, you must file it in paper form, with a request for confidential treatment, and you must follow the procedure explained in FTC Rule 4.9(c), 16 CFR 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comments to be withheld from the public record. Your comment will be kept confidential only if the FTC General Counsel grants your request in accordance with the law and the public interest.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comment online. To make sure that the Commission considers your online comment, you must file it at *https://ftcpublic.commentworks.com/ftc/safeguardsrulenprm* by following the instructions on the web-based form. If this document appears at *http://www.regulations.gov/#!home,* you also may file a comment through that Web site.

If you file your comment on paper, write ''Safeguards Rule, 16 CFR 314, Matter No. P145407'' on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW., Suite CC–5610 (Annex B), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW., 5th Floor, Suite 5610 (Annex B), Washington, DC 20024.

Visit the Commission Web site at *http://www.ftc.gov* to read this document and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before November 7, 2016. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *http://www.ftc.gov/ftc/privacy.htm.*

[18] *See* 65 FR 80,735 (Dec. 22, 2000) (determining the activity of ''finding'' to be an activity incidental to financial activity).

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 2016–21231 Filed 9–6–16; 8:45 am]

BILLING CODE 6750–01–P

DEPARTMENT OF JUSTICE

Drug Enforcement Administration

21 CFR Part 1308

[Docket No. DEA–440]

Schedules of Controlled Substances: Temporary Placement of U–47700 Into Schedule I

AGENCY: Drug Enforcement Administration, Department of Justice.

ACTION: Notice of intent.

SUMMARY: The Administrator of the Drug Enforcement Administration is issuing this notice of intent to temporarily schedule the synthetic opioid, 3,4-dichloro-*N*-[2-(dimethylamino)cyclohexyl]-*N*-methylbenzamide (also known as U–47700), into schedule I pursuant to the temporary scheduling provisions of the Controlled Substances Act. This action is based on a finding by the Administrator that the placement of this synthetic opioid into schedule I of the Controlled Substances Act is necessary to avoid an imminent hazard to the public safety. Any final order will impose the administrative, civil, and criminal sanctions and regulatory controls applicable to schedule I controlled substances under the Controlled Substances Act on the manufacture, distribution, possession, importation, exportation, research, and conduct of, instructional activities of this synthetic opioid.

DATES: September 7, 2016.

FOR FURTHER INFORMATION CONTACT: Michael J. Lewis, Office of Diversion Control, Drug Enforcement Administration; Mailing Address: 8701 Morrissette Drive, Springfield, Virginia 22152; Telephone: (202) 598–6812.

SUPPLEMENTARY INFORMATION: Any final order will be published in the **Federal Register** and may not be effective prior to October 7, 2016.

Legal Authority

The Drug Enforcement Administration (DEA) implements and enforces titles II and III of the Comprehensive Drug Abuse Prevention and Control Act of 1970, as amended. 21 U.S.C. 801–971. Titles II and III are referred to as the ''Controlled Substances Act'' and the ''Controlled Substances Import and Export Act,'' respectively, and are collectively referred to as the ''Controlled Substances Act'' or the ''CSA'' for the purpose of this action. The DEA publishes the implementing regulations for these statutes in title 21 of the Code of Federal Regulations (CFR), chapter II. The CSA and its implementing regulations are designed to prevent, detect, and eliminate the diversion of controlled substances and listed chemicals into the illicit market while providing for the legitimate medical, scientific, research, and industrial needs of the United States. Controlled substances have the potential for abuse and dependence and are controlled to protect the public health and safety.

Under the CSA, each controlled substance is classified into one of five schedules based upon its potential for abuse, its currently accepted medical use in treatment in the United States, and the degree of dependence the drug or other substance may cause. 21 U.S.C. 812. The initial schedules of controlled substances established by Congress are found at 21 U.S.C. 812(c), and the current list of all scheduled substances is published at 21 CFR part 1308.

Section 201 of the CSA, 21 U.S.C. 811, provides the Attorney General with the authority to temporarily place a substance into schedule I of the CSA for two years without regard to the requirements of 21 U.S.C. 811(b) if she finds that such action is necessary to avoid imminent hazard to the public safety. 21 U.S.C. 811(h)(1). In addition, if proceedings to control a substance are initiated under 21 U.S.C. 811(a)(1), the Attorney General may extend the temporary scheduling for up to one year. 21 U.S.C. 811(h)(2).

Where the necessary findings are made, a substance may be temporarily scheduled if it is not listed in any other schedule under section 202 of the CSA, 21 U.S.C. 812, or if there is no exemption or approval in effect for the substance under section 505 of the Federal Food, Drug, and Cosmetic Act (FDCA), 21 U.S.C. 355. 21 U.S.C. 811(h)(1). The Attorney General has delegated scheduling authority under 21 U.S.C. 811 to the Administrator of the DEA. 28 CFR 0.100.

Background

Section 201(h)(4) of the CSA, 21 U.S.C. 811(h)(4), requires the Administrator to notify the Secretary of the Department of Health and Human Services (HHS) of his intention to temporarily place a substance into schedule I of the CSA.[1] The Administrator transmitted notice of his intent to place U–47700 in schedule I on a temporary basis to the Assistant Secretary by letter dated April 18, 2016. The Assistant Secretary responded to this notice by letter dated April 28, 2016, and advised that based on review by the Food and Drug Administration (FDA), there are currently no investigational new drug applications or approved new drug applications for U–47700. The Assistant Secretary also stated that the HHS has no objection to the temporary placement of U–47700 into schedule I of the CSA. U–47700 is not currently listed in any schedule under the CSA, and no exemptions or approvals are in effect for U–47700 under section 505 of the FDCA, 21 U.S.C. 355. The DEA has found that the control of U–47700 in schedule I on a temporary basis is necessary to avoid an imminent hazard to public safety.

To find that placing a substance temporarily into schedule I of the CSA is necessary to avoid an imminent hazard to the public safety, the Administrator is required to consider three of the eight factors set forth in section 201(c) of the CSA, 21 U.S.C. 811(c): The substance's history and current pattern of abuse; the scope, duration and significance of abuse; and what, if any, risk there is to the public health. 21 U.S.C. 811(h)(3). Consideration of these factors includes actual abuse, diversion from legitimate channels, and clandestine importation, manufacture, or distribution. 21 U.S.C. 811(h)(3).

A substance meeting the statutory requirements for temporary scheduling may only be placed in schedule I. 21 U.S.C. 811(h)(1). Substances in schedule I are those that have a high potential for abuse, no currently accepted medical use in treatment in the United States, and a lack of accepted safety for use under medical supervision. 21 U.S.C. 812(b)(1).

U–47700

The substance U–47700 was first described in 1978 in the patent literature. Publications in the scientific literature in the early 1980's found that U–47700 behaved similarly to morphine in animal models. No approved medical

[1] As discussed in a memorandum of understanding entered into by the Food and Drug Administration (FDA) and the National Institute on Drug Abuse (NIDA), the FDA acts as the lead agency within the HHS in carrying out the Secretary's scheduling responsibilities under the CSA, with the concurrence of NIDA. 50 FR 9518, Mar. 8, 1985. The Secretary of the HHS has delegated to the Assistant Secretary for Health of the HHS the authority to make domestic drug scheduling recommendations. 58 FR 35460, July 1, 1993.