

**ACTION:** 30-Day notice and request for comments.

**SUMMARY:** The Peace Corps will submit the following information collection request to the Office of Management and Budget (OMB) for review and approval. In accordance with the Paperwork Reduction Act of 1995, we invite comments on this collection from all interested individuals and organizations. The purpose of this notice is to allow an additional 30 days for public comments.

**DATES:** Submit comments on or before June 30, 2022.

**ADDRESSES:** Comments should be addressed to Virginia Burke, FOIA/Privacy Act Officer. Virginia Burke can be contacted by email at [pcf@peacecorps.gov](mailto:pcf@peacecorps.gov). Email comments must be made in text and not in attachments.

**FOR FURTHER INFORMATION CONTACT:** Virginia Burke, FOIA/Privacy Act Officer, at (202) 692-1887, or [PCFR@peacecorps.gov](mailto:PCFR@peacecorps.gov).

**SUPPLEMENTARY INFORMATION:**

*Title:* Onboarding Form for Peace Corps Volunteer Applicants.

*OMB Control Number:* 0420-0563.

*Agency Form Number:* PC-2174.

*Type of Request:* Intent to seek reinstatement, with change, of a previously approved information collection for which approval has expired, for three years.

*Originating Office:* Office of Volunteer Recruitment and Selection.

*Affected Public:* This collection will request information from Peace Corps Volunteer applicants who are invited to join the Peace Corps.

*Respondents Obligation to Reply:* Voluntary.

*Burden to the Public:*

*Peace Corps Response Interview Assessment:*

(a) *Annual Estimated Number of Respondents:* 5,000.

(b) *Frequency of Response:* One time.

(c) *Estimated Average Burden per Response:* 60 minutes.

(d) *Annual estimated Total Reporting Burden:* 5,000 hours.

(e) *Estimated annual cost to respondents:* 0.00.

*General description of collection and purpose:* The Peace Corps uses the Onboarding Portal to collect essential administrative information from invitees for use during Peace Corps Volunteer service, including such information as first, middle and last name, birthdate, Social Security number, primary contact information, designated emergency contact names and contact information, legal history updates, direct deposit information

associated with a bank account, student loan history, and life insurance designations. The information is used by the Peace Corps to establish specific services for invitees for the purposes of supporting the Peace Corps Volunteer during service. The Information Collection expired on August 31, 2020, during the Corona Virus 2019 pandemic. We are seeking reinstatement with minor changes of this information collection and a three-year clearance.

*Request for Comment:* Peace Corps invites comments on whether the proposed collection of information is necessary for proper performance of the functions of the Peace Corps, including whether the information will have practical use; the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the information to be collected; and, ways to minimize the burden of the collection of information on those who are to respond, including through the use of automated collection techniques, when appropriate, and other forms of information technology.

This notice is issued in Washington, DC, on May 24, 2022.

**Virginia Burke,**

*FOIA/Privacy Act Officer, Management.*

[FR Doc. 2022-11524 Filed 5-27-22; 8:45 am]

**BILLING CODE 6051-01-P**

## OFFICE OF PERSONNEL MANAGEMENT

### President's Commission on White House Fellowships Advisory Committee: Closed Meeting

**AGENCY:** President's Commission on White House Fellowships, Office of Personnel Management.

**ACTION:** Notice of meeting.

**SUMMARY:** The President's Commission on White House Fellowships (PCWHF) was established by an Executive Order in 1964. The PCWHF is an advisory committee composed of Special Government Employees appointed by the President. The Advisory Committee meets in June to interview potential candidates for recommendation to become a White House Fellow.

The meeting is closed.

*Name of Committee:* President's Commission on White House Fellowships Selection Weekend.

*Date:* June 2-5, 2022.

*Time:* 7:00 a.m.—5:30 p.m.

*Place:* St. Regis Hotel, 16th and K Street, Washington, DC 20006.

*Agenda:* The Commission will interview 30 National Finalists for the

selection of the new class of White House Fellows.

**FOR FURTHER INFORMATION CONTACT:** Rosemarie Vela, 712 Jackson Place NW, Washington, DC 20503, Phone: 202-395-4522.

U.S. Office of Personnel Management.

**Stephen Hickman,**

*Federal Register Liaison.*

[FR Doc. 2022-11616 Filed 5-27-22; 8:45 am]

**BILLING CODE 6325-69-P**

## SECURITIES AND EXCHANGE COMMISSION

### Sunshine Act Meetings

**TIME AND DATE:** 2 p.m. on Thursday, June 2, 2022.

**PLACE:** The meeting will be held via remote means and/or at the Commission's headquarters, 100 F Street NE, Washington, DC 20549.

**STATUS:** This meeting will be closed to the public.

**MATTERS TO BE CONSIDERED:**

Commissioners, Counsel to the Commissioners, the Secretary to the Commission, and recording secretaries will attend the closed meeting. Certain staff members who have an interest in the matters also may be present.

In the event that the time, date, or location of this meeting changes, an announcement of the change, along with the new time, date, and/or place of the meeting will be posted on the Commission's website at <https://www.sec.gov>.

The General Counsel of the Commission, or his designee, has certified that, in his opinion, one or more of the exemptions set forth in 5 U.S.C. 552b(c)(3), (5), (6), (7), (8), 9(B) and (10) and 17 CFR 200.402(a)(3), (a)(5), (a)(6), (a)(7), (a)(8), (a)(9)(ii) and (a)(10), permit consideration of the scheduled matters at the closed meeting.

The subject matter of the closed meeting will consist of the following topics:

Institution and settlement of injunctive actions;

Institution and settlement of administrative proceedings;

Resolution of litigation claims; and

Other matters relating to examinations and enforcement proceedings.

At times, changes in Commission priorities require alterations in the scheduling of meeting agenda items that may consist of adjudicatory, examination, litigation, or regulatory matters.

**CONTACT PERSON FOR MORE INFORMATION:**

For further information; please contact

Vanessa A. Countryman from the Office of the Secretary at (202) 551-5400.

*Authority:* 5 U.S.C. 552b.

Dated: May 26, 2022.

**Vanessa A. Countryman,**  
Secretary.

[FR Doc. 2022-11737 Filed 5-26-22; 4:15 pm]

BILLING CODE 8011-01-P

## SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-94975; File No. SR-DTC-2022-004]

### Self-Regulatory Organizations; The Depository Trust Company; Notice of Filing of a Proposed Rule Change To Require Applicants and Members To Maintain or Upgrade Their Network or Communications Technology

May 24, 2022.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (“Act”)<sup>1</sup> and Rule 19-4 thereunder,<sup>2</sup> notice is hereby given that on May 11, 2022, The Depository Trust Company (“DTC”) filed with the Securities and Exchange Commission (“Commission”) the proposed rule change as described in Items I, II and III below, which Items have been prepared by the clearing agency. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

#### I. Clearing Agency’s Statement of the Terms of Substance of the Proposed Rule Change

The proposed rule change of DTC consists of modifications to Rules<sup>3</sup> to revise certain provisions in the Rules relating to the requirement of applicants for DTC membership, Participants and Pledgees, (collectively, “Participants”) of DTC, to require that each Participant upgrade its network technology, and communications technology or protocols to meet standards that DTC shall publish from time to time, as described in greater detail below.

#### II. Clearing Agency’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the clearing agency included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these

statements may be examined at the places specified in Item IV below. The clearing agency has prepared summaries, set forth in sections A, B, and C below, of the most significant aspects of such statements.

#### (A) Clearing Agency’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

##### 1. Purpose

DTC is proposing to adopt a requirement that each Participant provide documentation demonstrating that the Participant’s network technology, and communication technology or protocols meet the standards that DTC is currently requiring. The determination to require changes or upgrades is incorporated into DTC’s procedures and includes an evaluation of the external threat landscape, threats to DTC’s technology infrastructure and information assets, industry cybersecurity priorities, a review of the root causes of incidents, and an evaluation of the current state of the network infrastructure as expressed using third-party assessments. For existing Participants and Pledgees, a new requirement is being proposed to require such Participants to upgrade their network technology, and communication technology or protocols within the timeframe published by DTC. The proposed changes are described in greater detail below.

##### (i) Background of the Requirement

Currently, DTC does not require, either as part of its application for membership or as an ongoing membership requirement, any level or version for network technology, such as a web browser or other technology, or any level or version of communications technology or protocols, such as email encryption, secure messaging, or file transfers, that are being used to connect to or communicate with DTC. In the current environment, DTC maintains multiple network and communications methods and protocols, some either obsolete or many years older than the current standard in order to support Participants using these older technologies, which leaves communications between DTC and its Participants vulnerable to interception or the introduction of unknown entries, and requires DTC to expend additional resources, both in personnel and equipment, to maintain older communications channels. In addition, Participant’s use of older technology delays the implementation by DTC to upgrade its internal systems, which, by doing so, risks losing connectivity with

a number of Participants. Given DTC’s critical role in the marketplace, this is a risk that needs to be addressed.

DTC believes that it should require current network technology, and current communication technology and protocol standards for Participants connecting to its network. For example, The National Institute of Standards and Technology or NIST<sup>4</sup> Special Publication 800-52 revision 2, specifies servers that support government-only applications shall be configured to use TLS<sup>5</sup> 1.2 and should be configured to use TLS 1.3 as well. These servers should not be configured to use TLS 1.1 and shall not use TLS 1.0, SSL 3.0, or SSL 2.0.<sup>6</sup> The internet Engineer Task Force (“IETF”)<sup>7</sup> formally deprecated TLS versions 1.0 and 1.1 in March of 2021, stating, “These versions lack support for current and recommended cryptographic algorithms and mechanisms, and various government and industry profiles of applications using TLS now mandate avoiding these old TLS versions. . . . Removing support for older versions from implementations reduces the attack surface, reduces opportunity for misconfiguration, and streamlines library and product maintenance.”<sup>8</sup> TLS 1.0 (published in 1999) does not support many modern, strong cipher (encryption) suites and TLS 1.1 (published in 2006) is a security improvement over TLS 1.0 but still does not support certain stronger cipher or encryption suites.<sup>9</sup> Another communications technology, File Transfer Protocol (“FTP”) is considered an insecure protocol, because it transfers user authentication data (username and password) and file data as plain-text (not encrypted) over the network. This makes it highly vulnerable to sniffing attacks that allow an attacker to collect usernames and passwords from the network and inject malware into downloads via FTP. Following the guidance from NIST and

<sup>4</sup> The National Institute of Standards and Technology (“NIST”) is part of the U.S. Department of Commerce.

<sup>5</sup> Transport Layer Security (“TLS”), the successor of the now-deprecated Secure Sockets Layer (“SSL”), is a cryptographic protocol designed to provide communications security over a computer network.

<sup>6</sup> A government-only application is an application where the intended users are exclusively government employees or contractors working on behalf of the government. The full NIST publication is available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf>.

<sup>7</sup> The internet Engineering Task Force (“IETF”) is an open standards organization, which develops and promotes voluntary internet standards, in particular the technical standards that comprise the internet protocol suite (TCP/IP).

<sup>8</sup> <https://datatracker.ietf.org/doc/rfc8996/>.

<sup>9</sup> *Id.*

<sup>1</sup> 15 U.S.C. 78s(b)(1).

<sup>2</sup> 17 CFR 240.19b-4.

<sup>3</sup> Capitalized terms not defined herein are defined in the Rules, available at [https://dtcc.com/~media/Files/Downloads/legal/rules/DTC\\_rules.pdf](https://dtcc.com/~media/Files/Downloads/legal/rules/DTC_rules.pdf).