

**SUPPLEMENTARY INFORMATION:****I. Obtaining Information and Submitting Comments****A. Obtaining Information**

Please refer to Docket ID NRC–2022–0215 when contacting the NRC about the availability of information for this action. You may obtain publicly available information related to this action by any of the following methods:

- *Federal Rulemaking Website*: Go to <https://www.regulations.gov> and search for Docket ID NRC–2022–0215.

- *NRC's Agencywide Documents Access and Management System (ADAMS)*: You may obtain publicly available documents online in the ADAMS Public Documents collection at <https://www.nrc.gov/reading-rm/adams.html>. To begin the search, select "Begin Web-based ADAMS Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1–800–397–4209, 301–415–4737, or by email to [PDR.Resource@nrc.gov](mailto:PDR.Resource@nrc.gov). The draft ISG, "Material Compatibility for non-Light Water Reactors, DANU–ISG–2023–01" is available in ADAMS under Accession No. ML22203A175.

- *NRC's PDR*: You may examine and purchase copies of public documents, by appointment, at the NRC's PDR, Room P1 B35, One White Flint North, 11555 Rockville Pike, Rockville, Maryland 20852. To make an appointment to visit the PDR, please send an email to [PDR.Resource@nrc.gov](mailto:PDR.Resource@nrc.gov) or call 1–800–397–4209 or 301–415–4737, between 8 a.m. and 4 p.m. eastern time (ET), Monday through Friday, except Federal holidays.

**B. Submitting Comments**

The NRC encourages electronic comment submission through the Federal rulemaking website (<https://www.regulations.gov>). Please include Docket ID NRC–2022–0215 in your comment submission.

The NRC cautions you not to include identifying or contact information that you do not want to be publicly disclosed in your comment submission. The NRC will post all comment submissions at <https://www.regulations.gov> as well as enter the comment submissions into ADAMS. The NRC does not routinely edit comment submissions to remove identifying or contact information.

If you are requesting or aggregating comments from other persons for submission to the NRC, then you should inform those persons not to include identifying or contact information that they do not want to be publicly

disclosed in their comment submission. Your request should state that the NRC does not routinely edit comment submissions to remove such information before making the comment submissions available to the public or entering the comment into ADAMS.

**II. Background**

As part of its review of advanced non-light water reactor applications, the NRC determines whether materials proposed to be used will allow components to fulfill design requirements for the design life, or that adequate surveillance and monitoring programs are in place. NRC regulations in part 50 and part 52 of title 10 of the *Code of Federal Regulations* (10 CFR) include requirements for material qualification and performance monitoring. The NRC endorsed American Society of Mechanical Engineers (ASME) Code Section III, Division 5, "High Temperature Reactors" (Section III–5), with conditions, in Revision 2 of Regulatory Guide 1.87, "Acceptability of ASME Code, Section III, Division 5, 'High Temperature Reactors,'" (ADAMS Accession No. ML22101A263).

**III. Discussion**

The purpose of this draft ISG is to aid the NRC staff reviewing non-light water reactor applications for a construction permit or operating license under 10 CFR part 50 or for a design certification, combined license, standard design approval, or manufacturing license under 10 CFR part 52 that propose to use materials allowed under Section III–5. Section III–5 specifies the mechanical properties and allowable stresses to be used for design of components in high temperature reactors. Because Section III–5 states that it does not provide methods to evaluate deterioration that may occur in service as a result of corrosion, mass transfer phenomena, radiation effects, or other material instabilities, this draft ISG identifies information that the staff should consider as part of its review of a non-light water reactor application to review applicable design requirements including qualification and monitoring programs for safety-significant structures, systems, and components.

Dated: March 1, 2023.

For the Nuclear Regulatory Commission.

**Steven T. Lynch,**

*Chief, Advanced Reactor Policy Branch, Division of Advanced Reactors and Non-Power Production and Utilization Facilities, Office of Nuclear Reactor Regulation.*

[FR Doc. 2023–04577 Filed 3–6–23; 8:45 am]

**BILLING CODE 7590–01–P**

**OFFICE OF SCIENCE AND TECHNOLOGY POLICY****Request for Information; NSPM 33 Research Security Programs Standard Requirement**

**AGENCY:** Office of Science and Technology Policy (OSTP).

**ACTION:** Notice and request for comments.

**SUMMARY:** The Office of Science and Technology Policy (OSTP) requests comments from the public on draft Research Security Programs Standard Requirement developed in response to National Security Presidential Memorandum 33 on National Security Strategy for United States Government-Supported Research and Development (R&D). The draft Standard Requirement has been created by OSTP, together with Federal agencies and the Office of Management and Budget, to ensure that there is uniformity across Federal research agencies in implementing this requirement.

**DATES:** Interested persons and organizations are invited to submit comments on or before 5 p.m. ET June 5, 2023.

**ADDRESSES:** Submit comments electronically to [researchsecurity@ostp.eop.gov](mailto:researchsecurity@ostp.eop.gov) with the subject line *Comment on Research Security Programs* by the deadline. Due to time constraints, mailed paper submissions will not be accepted.

*Instructions:* Response to this notice is voluntary. Responses to this notice may be used by the government for program planning on a non-attribution basis. OSTP therefore requests that no business proprietary information or copyrighted information be submitted in response to this notice. Please note that the U.S. Government will not pay for response preparation, or for the use of any information contained in the response.

Responses may address one or as many topics as desired from the enumerated list provided in this request for comment, noting the corresponding number of the topic(s) to which the response pertains. Submissions must not exceed 5 pages (exclusive of cover page) in 12-point or larger font, with a page number provided on each page. Responses should include the name of the person(s) or organization(s) filing the comment, as well as the respondent type (e.g., academic institution, advocacy group, professional society, community-based organization, industry, member of the public, government, other). Respondent's role in the organization may also be

provided (e.g., researcher, administrator, student, program manager, journalist) on a voluntary basis.

Please also organize your responses such that substantive comments are at the beginning of the document and more procedural and/or technical comments are at the end. This format will help us to absorb and respond to your comments in a more organized way.

Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials; these materials, as well as a list of references, do not count toward the 5-page limit. No business proprietary information, copyrighted information, or personally identifiable information (aside from that requested above) should be submitted in response to this request for comment. Comments submitted in response to this notice are subject to the Freedom of Information Act. Comments submitted may be posted online or otherwise released publicly.

**FOR FURTHER INFORMATION CONTACT:**

Direct questions to Kei Koizumi at [researchsecurity@ostp.eop.gov](mailto:researchsecurity@ostp.eop.gov); tel: 202-456-4444.

**SUPPLEMENTARY INFORMATION:** National Security Presidential Memorandum 33 provides for a National Security Strategy for United States Government—Supported Research and Development. Section 4(g) directs that, “heads of funding agencies shall require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates a research security program. Institutional research security programs should include elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training.”

On January 4, 2022, the OSTP’s National Science and Technology Council released Guidance for Implementing National Security Presidential Memorandum 33 (NSPM–33). NSPM–33 charges OSTP with “coordinat[ing] activities to protect Federally funded R&D from foreign government interference, and outreach to the United States scientific and academic communities to enhance awareness of risks to research security and Federal Government actions to address these risks.” A similar charge is captured in the National Defense Authorization Act of 2020.<sup>1</sup>

The resulting Guidance, called for by the Director of OSTP, delivers on three key priorities, consistent with the values of the Biden-Harris Administration: (1) protecting America’s security AND openness; (2) being clear in our delivery of guidance and information to impacted communities, so that compliance with NSPM–33 is easy, straightforward, and minimally burdensome; and (3) ensuring that our policies do not fuel xenophobia or prejudice.

The Guidance also captured next steps regarding the implementation of a Standard Requirement for Research Security Programs (hereinafter shortened to ‘Standard Requirement’), stating on page 19: “OSTP, in consultation with the NSTC Subcommittee on Research Security, OMB, and external stakeholders, will develop a standardized requirement for uniform implementation across research agencies. Following a 90-day external engagement period, OSTP will complete the standardized requirement in the subsequent 120 days, and, upon completion, work with OMB to develop a plan to implement the standardized requirement. Upon receipt of the standards, relevant research agencies should engage with external stakeholders to ensure that program requirements are appropriate to the broad range of organizations that are subject to the requirement.”

In fulfillment of this statement, a draft Standard Requirement has been completed and is available for review at: [https://www.whitehouse.gov/wp-content/uploads/2023/02/RS\\_Programs\\_Guidance\\_public\\_comment.pdf](https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf).

To enable further coordination, OSTP is leading engagement with external stakeholders, as the Guidance described. This request for comment is an important source of engagement and is meant to give the public an opportunity to review and provide feedback on the draft Standard Requirement. Through this request for comment, OSTP seeks public input on the Standard Requirement, with special attention to equity, clarity, feasibility, burden, and compliance.

general.—The Director of the Office of Science and Technology Policy, acting through the National Science and Technology Council, in consultation with the National Security Advisor, shall establish or designate an interagency working group to coordinate activities to protect federally funded research and development from foreign interference, cyber attacks, theft, or espionage and to develop common definitions and best practices for Federal science agencies and grantees, while accounting for the importance of the open exchange of ideas and international talent required for scientific progression and American leadership in science and technology.”

*Scope:* OSTP invites comment from any interested stakeholders. In particular, OSTP is interested in input from research organizations that will be subject to the Research Security Program requirement, researchers within those organizations, professional organizations representing those organizations, and organizations representing diverse interests across the U.S. research ecosystem.

*Information Requested:* Respondents may provide information for one or more of the topics included below. Respondents are asked to note the corresponding number/s to which responses pertain.

1. *Equity.* The NSPM–33 implementation Guidance requires that research security policies and practices are implemented in an equitable and non-discriminatory fashion. Are there any areas of the Standard Requirement that have not, in your view, upheld the fundamental commitments to equity and non-discrimination?

2. *Clarity.* It is essential that the Research Security Programs Standard Requirement is clear. Clarity enables equity, transparency, and compliance. Comments on clarity throughout the Standard Requirement are especially appreciated, particularly as they pertain to the ability of organizations to understand and meet the provisions of the Standard Requirement. Your perspectives on the extent to which the Standard Requirement is clear and allows for straightforward adoption are of great interest.

3. *Feasibility.* The Research Security Program Standard Requirement will be most successful if covered organizations view adoption as feasible. With that in mind, are there aspects of the Standard Requirement that are concerning in terms of implementation? If so, how and why?

4. *Burden.* Closely related to feasibility is burden. Engagement with the research community has allowed us to understand that concerns about burden, whether in regard to financial or administrative burden, are high. Provisions in the Standard Requirement have been scoped with an aim to lessen burden, such as centralized certification on SAM.gov and technical assistance for development of research security training. Are there other measures that would help to lower the burden on the research community in implementing the Standard Requirement?

5. *Compliance.* The draft Standard Requirement suggests self-certification as the primary model of compliance with the requirements, with initially certification required one year after the issuance of the Standard Requirement.

<sup>1</sup> The language from the 2020 NDAA (Public Law 116–92), captured in Sec. 1746. (a), states: “In

What are your perspectives on these approaches? Are there others that should be considered?

Dated: March 2, 2023.

**Stacy Murphy,**

*Deputy Chief Operations Officer/Security Officer.*

[FR Doc. 2023-04660 Filed 3-6-23; 8:45 am]

BILLING CODE 3270-F1-P

## SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-97001; File No. SR-FICC-2023-003]

### Self-Regulatory Organizations; Fixed Income Clearing Corporation; Notice of Filing of Proposed Rule Change To Revise the Description of the Stressed Period Used To Calculate the Value-at-Risk Charge and Make Other Changes

March 1, 2023.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (“Act”)<sup>1</sup> and Rule 19b-4 thereunder,<sup>2</sup> notice is hereby given that on February 17, 2023, Fixed Income Clearing Corporation (“FICC”) 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<sup>3</sup> consists of amendments to the GSD Methodology Document—GSD Initial Market Risk Margin Model (“GSD QRM Methodology Document”)<sup>4</sup> and the

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

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

<sup>3</sup> Capitalized terms used herein and not defined shall have the meaning assigned to such terms in the FICC’s Government Securities Division (“GSD”) Rulebook (“GSD Rules”) and FICC’s Mortgage-Backed Securities Division (“MBSD”) Clearing Rules (“MBSD Rules”), and together with the GSD Rules, the “Rules”, available at <http://www.dtcc.com/legal/rules-and-procedures.aspx>.

<sup>4</sup> The GSD QRM Methodology Document was filed as a confidential exhibit in the rule filing and advance notice for GSD sensitivity VaR. See Securities Exchange Act Release Nos. 83362 (June 1, 2018), 83 FR 26514 (June 7, 2018) (SR-FICC-2018-001) and 83223 (May 11, 2018), 83 FR 23020 (May 17, 2018) (SR-FICC-2018-801). The GSD QRM Methodology has been subsequently amended. See Securities Exchange Act Release Nos. 85944 (May 24, 2019), 84 FR 25315 (May 31, 2019) (SR-FICC-2019-001), 90182 (October 14, 2020), 85 FR 66630 (October 20, 2020) (SR-FICC-2020-009), 93234 (October 1, 2021), 86 FR 55891 (October 7, 2021) (SR-FICC-2021-007), and 95605 (August 25,

MBSD Methodology and Model Operations Document—MBSD Quantitative Risk Model (“MBSD QRM Methodology Document”),<sup>5</sup> and collectively with the GSD QRM Methodology Document, the “QRM Methodology Documents”) in order to revise the description of the stressed period used to calculate the VaR Charge (as defined below). FICC is also proposing to amend the GSD QRM Methodology Document in order to clarify the language describing the floor parameters used for the calculation of the VaR Floor. In addition, FICC is proposing to amend the QRM Methodology Documents to make certain technical changes, 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

FICC has observed significant volatility in the U.S. government securities market due to tightening monetary policy, increasing inflation, and recession fears. The significant volatility has led to greater risk exposures for FICC. In order to mitigate the increased risk exposures, FICC has to quickly and timely respond to rapidly changing market conditions. For example, in order to respond to rapidly changing market conditions, FICC may need to quickly and timely adjust the look-back period that FICC uses for

2022), 87 FR 53522 (August 31, 2022) (SR-FICC-2022-005).

<sup>5</sup> The MBSD QRM Methodology was filed as a confidential exhibit in the rule filing and advance notice for MBSD sensitivity VaR. See Securities Exchange Act Release Nos. 79868 (January 24, 2017), 82 FR 8780 (January 30, 2017) (SR-FICC-2016-007) and 79843 (January 19, 2017), 82 FR 8555 (January 26, 2017) (SR-FICC-2016-801). The MBSD QRM Methodology has been amended. See Securities Exchange Act Release Nos. 85944 (May 24, 2019), 84 FR 25315 (May 31, 2019) (SR-FICC-2019-001), 90182 (October 14, 2020), 85 FR 66630 (October 20, 2020) (SR-FICC-2020-009), 92303 (June 30, 2021), 86 FR 35854 (July 7, 2021) (SR-FICC-2020-017) and 95070 (June 8, 2022), 87 FR 36014 (June 14, 2022) (SR-FICC-2022-002).

purposes of calculating the VaR Charge with an appropriate stressed period, as needed, to enable FICC to calculate and collect adequate margin from members. Accordingly, FICC is proposing to amend the QRM Methodology Documents by revising the description of the stressed period used to calculate the VaR Charge in order to enable FICC to quickly and timely adjust the look-back period used for calculating the VaR Charge with an appropriate stressed period, as needed. Adjustments to the look-back period could affect the amount of the VaR Charge that GSD Members are assessed by either increasing or decreasing such charge to reflect the level of risk the activities of the GSD Members presented to FICC.

FICC is also proposing to amend the GSD QRM Methodology Document in order to clarify the language describing the floor parameters used for the calculation of the VaR Floor. In addition, FICC is proposing to amend the QRM Methodology Documents to make certain technical changes.

FICC, through GSD and MBSD, serves as a central counterparty (“CCP”) and provider of clearance and settlement services for the U.S. government securities and mortgage-backed securities markets. A key tool that FICC uses to manage its credit exposures to its members is the daily collection of margin from each member. The aggregated amount of all GSD and MBSD members’ margin constitutes the GSD Clearing Fund and MBSD Clearing Fund (collectively referred to herein as the “Clearing Fund”), which FICC would be able to access should a defaulted member’s own margin be insufficient to satisfy losses to FICC caused by the liquidation of that member’s portfolio. Each member’s margin consists of a number of applicable components, including a value-at-risk (“VaR”) charge (“VaR Charge”) designed to capture the potential market price risk associated with the securities in a member’s portfolio. The VaR Charge is typically the largest component of a member’s margin requirement. The VaR Charge is designed to cover FICC’s projected liquidation losses with respect to a defaulted member’s portfolio at a 99% confidence level.

FICC calculates VaR Charge by using a methodology referred to as the sensitivity approach. The sensitivity approach leverages external vendor expertise in supplying the market risk attributes, which would then be incorporated by FICC into the GSD and MBSD models to calculate the VaR Charge. Specifically, FICC sources security-level risk sensitivity data and