*Name of Committee:* Center for Scientific Review Special Emphasis Panel; Member Conflict: Sensorimotor, Olfaction, and Interoception.

*Date:* November 21, 2024.

*Time:* 12 p.m. to 6 p.m.

*Agenda:* To review and evaluate grant applications.

*Address:* National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

*Meeting Format:* Virtual Meeting.

*Contact Person:* Kirk Thompson, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 5184, MSC 7844, Bethesda, MD 20892, 301–435–1242, email: *kgt@mail.nih.gov.*

*Name of Committee:* Center for Scientific Review Special Emphasis Panel; Member Conflict: Skeletal Muscle and Rehabilitation Sciences.

*Date:* November 22, 2024.

*Time:* 9 a.m. to 6 p.m.

*Agenda:* To review and evaluate grant applications.

*Address:* National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

*Meeting Format:* Virtual Meeting.

*Contact Person:* Chee Lim, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 4128, Bethesda, MD 20892, (301) 435–1850, email: *limc4@csr.nih.gov.*

(Catalogue of Federal Domestic Assistance Program Nos. 93.306, Comparative Medicine; 93.333, Clinical Research, 93.306, 93.333, 93.337, 93.393–93.396, 93.837–93.844, 93.846–93.878, 93.892, 93.893, National Institutes of Health, HHS)

Dated: October 24, 2024.

**Bruce A. George,**

*Program Analyst, Office of Federal Advisory Committee Policy.*

[FR Doc. 2024–25099 Filed 10–28–24; 8:45 am]

**BILLING CODE 4140–01–P**

## DEPARTMENT OF HOMELAND SECURITY

**[Docket No. CISA–2024–0028]**

### Request for Comment on Product Security Bad Practices Guidance

**AGENCY:** Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

**ACTION:** Notice of availability; extension of comment period.

**SUMMARY:** On October 16, 2024, the Cybersecurity Division (CSD) within the Cybersecurity and Infrastructure Security Agency (CISA) published a request for comment in the **Federal Register** on the voluntary, draft Product Security Bad Practices guidance, which requests feedback on the draft guidance. CISA is extending the comment period for the draft guidance for an additional fourteen days through December 16, 2024.

**DATES:** The comment period for the proposed voluntary guidance published on October 16, 2024, at 89 FR 83508 is extended. Comments and related materials must be submitted on or before December 16, 2024.

**ADDRESSES:** You may submit comments, identified by docket number CISA–2024–0028, by following the instructions below for submitting comments via the Federal eRulemaking Portal at *https://www.regulations.gov.*

*Instructions:* All comments received must include the agency name and docket number Docket Number CISA–2024–0028. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided. CISA reserves the right to publicly republish relevant and unedited comments in their entirety that are submitted to the docket. Do not include personal information such as account numbers, social security numbers, or the names of other individuals. Do not submit confidential business information or otherwise sensitive or protected information.

*Docket:* For access to the docket to read the draft Product Security Bad Practices Guidance or comments received, go to *https://www.regulations.gov.*

**FOR FURTHER INFORMATION CONTACT:** Kirk Lawrence, 202–617–0036, *SecureByDesign@cisa.dhs.gov.*

**SUPPLEMENTARY INFORMATION:** On October 16, 2024, CISA published a request for comment on voluntary, draft Product Security Bad Practices guidance (89 FR 83508). In the draft guidance, we provided an overview of product security practices that are deemed exceptionally risky, particularly for organizations supporting critical infrastructure or national critical functions (NCFs), and it provides recommendations for software manufacturers to voluntarily mitigate these risks. The guidance contained in the document is non-binding, and while CISA encourages organizations to avoid these bad practices, the document imposes no requirement on them to do so. The draft guidance is scoped to software manufacturers who develop software products and services, including on-premises software, cloud services, and software as a service (SaaS), used in support of critical infrastructure or NCFs. The request for comment provided for a 45-day comment period, set to close on December 2, 2024. CISA received requests to extend the deadline given the Thanksgiving holiday. Therefore, the comment period is now open through December 16, 2024.

This notice is issued under the authority of 6 U.S.C. 652 and 659.

**Jeffrey E. Greene,**

*Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.*

[FR Doc. 2024–25078 Filed 10–28–24; 8:45 am]

**BILLING CODE 9111–LF–P**

## DEPARTMENT OF HOMELAND SECURITY

**[Docket No. CISA–2024–0029]**

### Request for Comment on Security Requirements for Restricted Transactions Under Executive Order 14117

**AGENCY:** Cybersecurity and Infrastructure Security Agency (CISA), DHS.

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

**SUMMARY:** CISA seeks public input on the development of security requirements for restricted transactions as directed by Executive Order (E.O.) 14117, ''Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern.'' E.O. 14117 addresses national-security and foreign-policy threats that arise when countries of concern and covered persons can access bulk U.S. sensitive personal data or government-related data. The proposed CISA security requirements for restricted transactions would apply to classes of restricted transactions identified in regulations issued by the Department of Justice (DOJ).

**DATES:** Written comments are requested on or before November 29, 2024.

**ADDRESSES:** You may send comments, identified by docket number CISA–2024–0029, through the Federal eRulemaking Portal available at *http://www.regulations.gov.*

*Instructions:* All comments received will be posted to *https://www.regulations.gov,* including any personal information provided. For detailed instructions on sending comments and for information on the types of comments that are of particular interest to CISA, see the ''Public Participation'' and ''Request for Public Input'' heading of the **SUPPLEMENTARY INFORMATION** section of this document. Please note that this notice and request

for comment is not a rulemaking and that the Federal eRulemaking Portal is being utilized only as a mechanism for receiving comments.

**FOR FURTHER INFORMATION CONTACT:** Alicia Smith, Senior Policy Counsel, Cybersecurity and Infrastructure Security Agency, *EOSecurityReqs@cisa.dhs.gov,* 202–316–1560.

**SUPPLEMENTARY INFORMATION:**

## I. Public Participation

All interested stakeholders are invited to comment on this notice and the security requirements described herein by submitting written data, comments, views, or arguments using the method identified in the **ADDRESSES** section. Interested stakeholders may view a copy of the proposed security requirements on CISA's website by visiting *https://www.cisa.gov* and searching for ''Proposed Security Requirements for Restricted Transactions.'' A copy of the proposed security requirements is also included in the docket for this notice and request for comment, docket number CISA–2024–0029. All members of the public are invited to comment including, but not limited to, specialists in the field, academic experts, industry stakeholders, and public interest groups.

*Instructions:* All submissions must include the agency name and Docket ID for this notice. Comments may be submitted electronically via the Federal e-Rulemaking Portal.

To submit comments electronically:

1. Go to *www.regulations.gov* and enter CISA–2024–0029 in the search field,

2. Click the ''Comment Now!'' icon, complete the required fields, and

3. Enter or attach your comments.

All submissions, including attachments and other supporting materials, will become part of the public record and may be subject to public disclosure. CISA reserves the right to publish relevant comments publicly, unedited and in their entirety. Personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Do not submit confidential business information or otherwise sensitive or protected information. All comments received will be posted to *http://www.regulations.gov.* Commenters are encouraged to identify the number of the specific topic or topics that they are addressing.

*Docket:* For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* and search for the Docket ID.

## II. Background

### *A. History and Legal Authority*

On February 28, 2024, the President issued E.O. 14117 entitled ''Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern'' (the ''Order''), pursuant to his authority under the Constitution and laws of the United States, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), and section 301 of Title 3, United States Code. In the Order, the President expanded the scope of the national emergency declared in E.O. 13873 of May 15, 2019 ''Securing the Information and Communications Technology and Services Supply Chain,'' and further addressed the national emergency with additional measures in E.O. 14034 of June 9, 2021, ''Protecting Americans' Sensitive Data from Foreign Adversaries.'' Specifically, Section 2(a) of E.O. 14117 directs the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, to issue, subject to public notice and comment, regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest (''transaction''), where the transaction: (i) involves bulk sensitive personal data or United States Government-related data, as defined by final rules implementing the Order; (ii) is a member of a class of transactions that has been determined by the Attorney General to pose an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access bulk sensitive personal data or United States Government-related data in a manner that contributes to the national emergency described in the Order; and (iii) meets other criteria specified by the Order.[1]

Among other things, the E.O., at Section 2(c) instructs the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the relevant agencies, to issue regulations identifying specific categories of transactions (''restricted transactions'') that meet the criteria described in (ii) above for which the Attorney General determines that security requirements, to be established by the Secretary of Homeland Security through the Director of CISA in accordance with Section 2(d) of the Order, adequately mitigate the risks of access by countries of concern or covered persons[2] to bulk sensitive personal data or United States Government-related data. In turn, Section 2(d) directs the Secretary of Homeland Security, acting through the Director of CISA, to propose, seek public comment on, and publish those security requirements, and Section 2(e) delegates to the Secretary of Homeland Security the President's powers under IEPPA as necessary to carry out Section 2(d).

On March 5, 2024, DOJ published an advance notice of proposed rulemaking (ANPRM) explaining a proposed framework that DOJ is considering for its forthcoming rules that would regulate certain data transactions involving bulk U.S. sensitive personal data and government-related data, as DOJ proposed to define these terms in the ANPRM. 89 FR 15780. The ANPRM states that DOJ is considering identifying three classes of restricted data transactions to address critical risk areas to the extent they involve countries of concern or covered persons and bulk U.S. sensitive personal data: vendor agreements; employment agreements; and investment agreements. 89 FR 15783. If implemented as described, such categories of transactions would be restricted, and otherwise prohibited unless they meet the security requirements developed by DHS in coordination with DOJ. *See* 89 FR 15788. The ANPRM includes an outline of what the security requirements might entail. 89 FR 15795. Through the ANPRM, DOJ also proposes a framework for enforcement of its regulations. *See* 89 FR 15797–15798.

DOJ is issuing a notice of proposed rulemaking (NPRM), Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, [DOJ Docket No. NSD–104, RIN 1124–AA01], in the proposed rule section of this issue of the **Federal Register** for public comment. Through this notice, CISA announces the proposed security requirements applicable to the classes of restricted transactions defined in DOJ's

[1] The other criteria do not directly impact the development of the security requirements but are related to DOJ's implementation of the E.O.'s directive via their regulations. *See* E.O. 14117, sec. 2(a)(iii)–(v), 89 FR 15421, 15423 (Mar. 1, 2024).

[2] Section 2(c)(iii) of the Order requires the Attorney General to identify, with the concurrence of the Secretaries of State and Commerce, countries of concern and, as appropriate, classes of covered persons for the purposes of the Order.

NPRM and requests public comment on the content of the security requirements.

*B. Purpose and Structure of Proposed Security Requirements*

The primary goal of the proposed security requirements is to address national-security and foreign-policy threats that arise when countries of concern [3] and covered persons access bulk U.S. sensitive personal data or U.S. government-related data that may be implicated by the categories of restricted transactions. As explained in E.O. 14117, unrestricted transfers of Americans' bulk sensitive personal data and U.S. government-related data to countries of concern present a range of threats to national security and foreign policy. *See* 89 FR 15421. Access to bulk sensitive personal data and government-related data can allow countries of concern to engage in malicious cyber-enabled activities and malign foreign influence. *See* 89 FR 15422. With access to such data, countries of concern can track and build profiles on U.S. individuals, including members of the military and Federal employees and contractors, for illicit purposes such as blackmail and espionage. *Id.* Countries of concern can also use access to this data to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities to intimidate them; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties. *Id.* In making this assessment, DOJ noted that the Office of the Director of National Intelligence (ODNI) has assessed that adversaries view data, including personally identifiable information on U.S. citizens, ''as a strategic resource'' to increase the effectiveness of their espionage, influence, kinetic, and cyber-attack operations and provide a strategic advantage over the United States. *See id.* (citing Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* at 26 (Feb. 6, 2023), *https://perma.cc/4B2Y-7NVD*). DOJ assessed that advanced technologies, including big-data analytics, artificial intelligence, and high-performance computing, increase the ability of countries of concern to analyze and manipulate large tranches of data to more effectively target, influence, and coerce people in the United States. *See* 89 FR 15781 and E.O. 14117.

The proposed security requirements are designed to mitigate the risk of sharing bulk U.S. sensitive personal data or U.S. government-related data with countries of concern or covered persons through restricted transactions.[4] They do this by imposing conditions specifically on the *covered data* that may be shared as part of a restricted transaction, on the *covered systems* more broadly (both terms CISA is proposing to define within the security requirements), and on the organization as a whole. While the proposed requirements on covered systems and on an organization's governance of those systems apply more broadly than to the data at issue and the restricted transaction itself, CISA assesses that implementation of these requirements is necessary to validate that the organization has the technical capability and sufficient governance structure to appropriately select, successfully implement, and continue to apply the proposed covered data-level security requirements in a way that addresses the risks identified by DOJ for the restricted transactions. For example, to ensure and validate that a covered system denies covered persons access to covered data, it is necessary to maintain audit logs of accesses as well as organizational processes to utilize those logs. Similarly, it is necessary for an organization to develop identity management processes and systems to establish an understanding of which persons may have access to different data sets.

In addition to proposed requirements on covered systems, applying security requirements on the covered data itself that may be accessed in a restricted transaction is also necessary to address the risks. The specific requirements that are most technologically and logistically appropriate for different types of restricted transactions may vary. For example, some transactions may be amenable to approaches that minimize data or process it in such a way that does not reveal covered data to covered persons. In other cases, techniques such as access control and encryption may be more appropriate to deny any access by covered persons to covered data. The proposed security requirements contemplate multiple options to minimize the risk to covered data, though all the options build upon the foundation of the proposed requirements imposed on covered systems and the organization as a whole. While CISA is proposing that U.S. persons [5] engaging in restricted transactions must implement all the organizational and covered-system level requirements, CISA proposes that such persons will have some flexibility to determine which combination of data-level requirements are sufficient to fully and effectively prevent access to covered data by covered persons and/or countries of concern, based on the nature of the transaction and the data at issue.

The proposed security requirements are divided into two sections: organizational and covered system-level requirements (Section I) and covered data-level requirements (Section II). The listed requirements were selected with the intent of directly mitigating the risk of access to covered data, with additional requirements included to ensure effective governance of that access, as well as approaches for establishing an auditable basis for compliance purposes. Requirements that directly mitigate the risk of access include I.B.1–2, I.B.4–6, and all data-level requirements (II.A.1–3, II.B.1–3, II.C, and II.D). Requirements included as a mechanism for ensuring proper implementation and governance of those access controls include I.A.1–7. Additional requirements incorporated as a mechanism for ensuring auditable compliance of the aforementioned access controls include I.B.3 and I.C. These proposed requirements reflect a minimum set of practices that CISA believes are required for effective data

[3] Terms used in CISA's proposed security requirements that are defined in the DOJ rulemaking have the same meaning in the proposed security requirements as provided in the DOJ rulemaking.

[4] CISA notes that the proposed security requirements are, as required by the E.O., designed to ''address the unacceptable risk posed by restricted transactions, as identified by the Attorney General.'' E.O. 14117 Sec. 2(d). They are not intended to reflect a comprehensive cybersecurity program. For example, several areas addressed in CISA's Cross-Sector Cybersecurity Performance Goals (CPGs), available at *https://www.cisa.gov/cross-sector-cybersecurity-performance-goals,* are not reflected in the proposed data security requirements, even though the CPGs themselves are a common set of protections that CISA recommends all critical infrastructure entities voluntarily implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. As the operational lead for federal cybersecurity and national coordinator for critical infrastructure security and resilience, CISA recommends that all U.S. persons implement cybersecurity best practices in light of the risk and potential consequence of cyber events.

[5] As noted above, for the purposes of the proposed security requirements, to the extent CISA uses a term that is proposed to be defined in the DOJ rulemaking, CISA proposes to use that definition. Therefore, CISA is using the term U.S. persons as proposed to be defined by the DOJ [A]NPRM. That definition reads ''any United States citizen, national, or lawful permanent resident; or any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; or any *entity* organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any *person* in the United States.'' 89 FR 15788 and proposed 28 CFR 202.257.

protection, as informed by CISA's operational experience. Through this notice, CISA seeks additional input based on the experience industry stakeholders. These requirements have been designed to be representative of broadly accepted industry best practices and are intended to address the needs of national security without imposing an unachievable burden on industry.

As directed by E.O. 14117, the proposed security requirements are based on National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF), and the NIST Privacy Framework (PF). 89 FR 15424. See NIST, Cybersecurity Framework ver. 2.0, available at *https://www.nist.gov/cyberframework,* and NIST, Privacy Framework ver. 1.0, available at *https://www.nist.gov/privacy-framework.* CISA has also leveraged existing performance goals, guidance, practices, and controls, including the CISA Cross-Sector Cybersecurity Performance Goals (CPGs), which are themselves based on the NIST CSF and PF. CISA, Cross-Sector Cybersecurity Performance Goals, available at *https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.* By leveraging existing performance goals, guidance, practices, and controls, CISA hopes to mitigate the burden of understanding and implementing the security requirements where necessary. In the proposed security requirements, CISA included parentheticals noting the specific NIST CSF and PF provisions upon which the proposed security requirements are based. CISA is seeking additional public comment on these references.

The DOJ NPRM proposes to require, consistent with E.O. 14117, that United States persons engaging in restricted transactions must comply with the final security requirements by incorporating the standards by reference.

Finally, the proposed security requirements include a definitions section. To the extent the proposed requirements use a term already proposed to be defined in the DOJ rulemaking, CISA's use of that term in the proposed security requirement would carry the same meaning. For the purpose of these proposed security requirements, CISA proposes to include definitions for six terms used exclusively in the proposed security requirements:

• *Asset.* CISA proposes to define the term to mean data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes. This proposed definition is derived from the CSF NIST CSF version 1.1, which defined asset as ''[t]he data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes.''

• *Covered data.* CISA proposes to define the term to mean the two categories of data identified by the E.O. and that DOJ is proposing to regulate—bulk U.S. sensitive personal data or government-related data.

• *Information system.* CISA proposes to define this term consistent with the definition in the Paperwork Reduction Act (PRA), 44 U.S.C. 3502.[6] The term would mean a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

• *Covered system.* CISA proposes to define this term as a specific type of information system that is used to conduct a number of activities related to covered data as part of a restricted transaction. These activities are drawn from a combination of the activities in the proposed definition of *information system* in the proposed security requirements and the activities in the DOJ ANPRM's proposed definition of *access. See* 89 FR 15788; proposed 28 CFR 202.201. The term would mean an information system used to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, view, receive, collect, process, maintain, use, share, disseminate, or dispose of covered data as part of a restricted transaction, regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified.

• *Network.* CISA proposes to define this term, which CISA developed consistent with the definition of the term in NIST Special Publication 800–171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The term would mean* a system of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

[6] 6 U.S.C. 650(14) (which applies to all of Title XXII of the Homeland Security Act of 2002, which, in turn, contains most of CISA's authorities) defines Information System as having the meaning given the term in the Paperwork Reduction Act, 44 U.S.C. 3502, and specifically includes ''industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.'' 6 U.S.C. 650(14). However, given CISA's assumption that this type of operational technology is unlikely to be implicated by DOJ's proposed regulations, CISA is not proposing to include the operational technology-related prong here. CISA welcomes comments on this assumption.

## III. Request for Public Input

### *A. Importance of Public Feedback*

CISA is committed to seeking and incorporating public input into its approach to the development and content of the security requirements required by E.O. 14117. The proposed security requirements are available for review on CISA's website by visiting *https://www.cisa.gov* and searching for ''Proposed Security Requirements for Restricted Transactions.'' A copy of the proposed security requirements is also included in the docket for this notice and request for comment, docket number CISA–2024–0029. Below is a list of questions regarding the proposed security requirements for which CISA believes feedback could be particularly useful. CISA seeks a balanced approach to development of the security requirements, which would mitigate the risks of access to Americans' bulk sensitive personal data or government-related data by countries of concern while accounting for the impact that adopting these measures may have on those entities that would implement them. CISA encourages public comment on these topics and any other topics that commenters believe may be useful to CISA in the development of the forthcoming security requirements. The type of feedback that is most useful to the agency will identify specific approaches that CISA may want to consider and provide information supporting why the approach would foster a cost-effective and balanced approach. As discussed in more detail below, commenters may want to consider submitting views on organizational- and system-level requirements and/or data-level requirements. Feedback that contains specific information, data, or recommendations is more useful to CISA than generic feedback that omits these components. For comments that contain any numerical estimates, CISA encourages the commenter to provide any assumptions made in calculating the numerical estimates.

### *B. List of Questions for Commenters*

Below is a non-exhaustive list of questions that are meant to assist members of the public in formulating their comments in response to this notice. The list of questions is not intended to restrict the issues that commenters may address. For more information on the proposed regulatory structure in which the security requirements will apply, please review DOJ's NPRM, Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related

Data by Countries of Concern or Covered Persons, [DOJ Docket No. NSD–104, RIN 1124–AA01], published in today's proposed rule section of the **Federal Register** for public comment.

1. Are the proposed security requirements sufficiently robust to mitigate the risks of access to Americans' bulk sensitive personal data or government-related data by countries of concern?

2. Are the proposed organizational- and system-level requirements sufficient to provide U.S. persons engaging in restricted transactions confidence that logical and physical access to covered data is sufficiently managed to deny access to covered persons or countries of concern?

3. Do the security requirements provide sufficient flexibility, clarity, and specificity for the types of restricted transactions typically engaged in by U.S. entities, including to avoid overly burdening commercial activity not involving covered data while providing sufficient level of detail to aid in compliance verification?

4. Are there other data-level requirements (beyond those listed in Section II of the proposed security requirements) that CISA should consider that would enable U.S. entities to engage in commercial transactions without revealing covered data to covered persons or countries of concern?

5. The current approach allows for flexibility to determine which data-level requirements are sufficient to fully and effectively prevent access to covered data by covered persons and/or countries of concern. Are there data-level requirements that CISA should consider requiring in all cases?

6. What additional interpretive guidance would be helpful to U.S. entities in determining which data-level requirements should be applied based on the nature of the transaction and the data at issue?

7. What substantive requirements should CISA consider in Section II.C. to further define appropriate privacy-enhancing technologies that may be used within restricted transactions?

8. Should the standards for data aggregation in Section II.A differ from the proposed definition of bulk in the DOJ regulations? If so, are there requirements CISA should impose for U.S. persons engaged in restricted transactions to ensure that covered data is not re-constructable through aggregation while permitting more granular thresholds?

9. Are there additional substantive standards that should be added to the data-level requirements in Section II to better ensure their implementation can achieve the policy goal of not permitting access to covered data by covered persons or countries of concern?

10. To what extent could the measures described currently be reversed, broken, or circumvented by a technologically sophisticated actor? Are there additional conditions that would better or more appropriately mitigate this risk? If so, please describe them in detail.

11. To what extent could the measures described be rendered reversible, breakable, or able to be circumvented by anticipated future technology advances? What type of future technology advances would pose the greatest risk to these types of protective measures?

12. Would it be useful to the entities likely to undertake restricted transactions if CISA mapped these requirements to ISO–27001 or example controls from NIST Special Publication 800–171 (*e.g.,* to facilitate compliance audits)?

**Jennie M. Easterly,**

*Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.*

[FR Doc. 2024–24709 Filed 10–22–24; 4:15 pm]

**BILLING CODE 9111–1LF–P**

## DEPARTMENT OF THE INTERIOR

### Fish and Wildlife Service

**[FWS–HQ–MB–2024–N056; FXMB1231099BPP0–256–FF09M22000; OMB Control Number 1018–0067]**

### Agency Information Collection Activities; Submission to the Office of Management and Budget; Approval Procedures for Nontoxic Shot and Shot Coatings

**AGENCY:** Fish and Wildlife Service, Interior.

**ACTION:** Notice of information collection; request for comment.

**SUMMARY:** In accordance with the Paperwork Reduction Act of 1995, we, the U.S. Fish and Wildlife Service (Service), are proposing to renew an information collection without change.

**DATES:** Interested persons are invited to submit comments on or before November 29, 2024.

**ADDRESSES:** Written comments and recommendations for the proposed information collection should be submitted within 30 days of publication of this notice at *https://www.reginfo.gov/public/do/PRAMain.* Find this particular information collection by selecting ''Currently under Review—Open for Public Comments'' or by using the search function. Please provide a copy of your comments to the Service Information Collection Clearance Officer, U.S. Fish and Wildlife Service, MS: PRB (JAO/3W), 5275 Leesburg Pike, Falls Church, VA 22041–3803 (mail); or by email to *Info_Coll@fws.gov.* Please reference ''1018–0067'' in the subject line of your comments.

**FOR FURTHER INFORMATION CONTACT:** Madonna L. Baucum, Service Information Collection Clearance Officer, by email at *Info_Coll@fws.gov,* or by telephone at (703) 358–2503. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

**SUPPLEMENTARY INFORMATION:** In accordance with the Paperwork Reduction Act (PRA; 44 U.S.C. 3501 *et seq.*) and its implementing regulations at 5 CFR 1320, all information collections require approval under the PRA. We may not conduct or sponsor and you are not required to respond to a collection of information unless it displays a currently valid OMB control number.

As part of our continuing effort to reduce paperwork and respondent burdens, we invite the public and other Federal agencies to comment on new, proposed, revised, and continuing collections of information. This helps us assess the impact of our information collection requirements and minimize the public's reporting burden. It also helps the public understand our information collection requirements and provide the requested data in the desired format.

On August 7, 2024, we published in the **Federal Register** (89 FR 64476) a notice of our intent to request that OMB renew this information collection. In that notice, we solicited comments for 60 days, ending on October 7, 2024. In a continued effort to increase public awareness of, and participation in, our public commenting processes associated with information collection requests, the Service also published the **Federal Register** notice on *Regulations.gov* (Docket No. FWS–HQ–MB–2024–0093) to provide the public with an additional method to submit comments (in addition to the typical U.S. mail submission method). We received an