OMB Control Number: 2535-XXXX

Expiration date: XX-XX-XXXX

The U.S. Department of Housing and Urban Development (HUD)

Office of the Chief Procurement Officer (OCPO)

Supply Chain Risk Management Questionnaire Version 1.1

June 2025

Responses to this document contain contractor bid or proposal information for official use by the United States Department of Housing and Urban Development only. It shall not be duplicated, used, or disclosed in whole or in part without prior written permission from the Office of Chief Information Officer (OCIO).

Paperwork Reduction Act Statement

Public Reporting Burden Statement

The public reporting burden for this collection of information is estimated to average 6 hours per response totaling 1,180 hours per annum, including the time for reviewing instructions, searching existing data sources, gathering, and maintaining the data needed, and completing and reviewing the collection of information. This 6 hour interval will consist of 4 hours for the initial completion and submission and 2 hours for each annual resubmission of the Questionnaire.of the Comments regarding the accuracy of this burden estimate and any suggestions for reducing this burden can be sent to U.S. Department of Housing and Urban Development, Office of the Chief Data Officer, R, 451 7th St SW, Room 8210, Washington, DC 20410-5000 or email: PaperworkReductionActOffice@hud.gov. **Do not send completed forms to this address.** This agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the collection displays a valid OMB control number. HUD collects this information to assess the landscape of current and future vendors to understand what supply chain risks are present in their ICT and procurement processes. HUD uses this information to assist in evaluating contractors' internal supply chain risk management program. This information is voluntary.

Authority: In accordance with Executive Order 14017, *America's Supply Chains*; Executive Order 14028, *Improving the Nation's Cybersecurity*; the Federal Acquisition Supply Chain Security Act (FASCSA); and incorporating guidance published in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161, Cyber Security Supply Chain Risk Management Practices for Systems and Organizations; the U.S. Department of Housing and Urban Development (HUD) has implemented a department-wide supply chain risk management (SCRM) program.

Additionally, FASCSA grants heads of Executive Branch departments and agencies the authority to evaluate the supply chain risk management practices of its vendors, including performing supply chain risk assessments of its vendors supplying information and communications technology (ICT) products or services. Further, FASCSA authorizes heads of agencies, and in extension Contracting Officers, to prioritize vendor risk assessments prior to procuring ICT products or services related to mission critical systems, critical software, and mission essential functions.

Purpose: The risk assessment enables HUD to assess the landscape of current and future vendors to understand what supply chain risks are present in their ICT and procurement processes. This Questionnaire assists HUD in evaluating the strength of its contractors' Supply

Chain Risk Management programs and aids the Acquisition Workforce in making informed decisions regarding procurement actions.

Background: Using guidance from the key documents, as well as preparation between key stakeholders and the SCRM Program Team, HUD is implementing an enterprise-wide SCRM Program. This initiative will include updated and applicable policy, procedures, and documentation that present the structure of the HUD SCRM Program and establish the guidance for performing vendor supply chain risk assessments. The HUD SCRM Program enables the department to implement executive orders, legal authorities, regulatory orders, and federal guidance which includes a consistent process for identifying supply chain risk in current and future vendor relationships.

HUD expects only minimal (if any) impact of this data collection on small business entities. HUD delivers this Questionnaire to ICT vendors and contractors equally. The SCRM Questionnaire will also minimize the burden by having pre-populated responses sections as well as instructions for how to fill out the response areas.

HUD makes every effort to maintain to protect vendor information, to the extent possible. The information collected may be considered contractor bid or proposal information, and as such may be subject to the requirements for disclosure, protection, and marking of proprietary and source selection information set forth in FAR Subpart 3.1 and 3.104.

This questionnaire is used to assess the supply chain risks associated with your company prior to engaging in a contract. HUD requires potential vendors to complete and submit this form, along with any supporting documentation, in response to our solicitation.

1. Vendor Information	
Complete this table with general information about your company.	
Date of Submission *(mm/dd/yy)*	
Vendor Name	
Description of Vendor	
Description of Services	
Legal Entity Type (e.g., Corporation, Limited Liability Company [LLC], Partnership, Sole Proprietorship)	
Website URL	
Vendor Address	
Vendor Unique Entity ID (UEI)	

2. Prior Survey Submission

Vendors supporting HUD's mission essential functions must provide an updated form every 12 months. All other vendors must submit once every three (3) years.

If you have submitted this form within the required timeframe (e.g., either 12 months or 3 years) and there have been no changes to any sections of this form, complete page one and two and submit with the rest of your solicitation package.

Following submission, inform your HUD contact that you have completed this questionnaire and all information is accurate and up to date.

☐ [Company Name] has submitted this SCRM Questionnaire within the past 12 months, and there have been no changes since the previous submission.

☐ [Company Name] has submitted this SCRM Questionnaire within the past 3 years, and there have been no changes since the previous submission.
[Text Box for HUD contact]

3. Vendor Key Business Relationship Contacts

Fill out the following information regarding key business relationship contacts from your company. We require at minimum, a contracting office representative or designee, general solicitation POC, or technical POC.

Name	Role	Email

4. Software Producer Self-Attestation Requirements

Fill out this section if your company is a software producer. If not, then please proceed to Section 5.

To be in accordance with the updated secure software development self-attestation requirements for software producers contained within the M-22-18 (Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, September 14, 2022) and M-23-16 (Update to Memorandum M-22-18, June 9, 2023), please provide the following information.

1. Has the software producer submitted a Secure Software Development Attestation Form ("Common Form") online to CISA's Repository for Software Attestations and Artifacts?	[Yes/No]

If yes, please proceed to question 2 in this section.	
1a. If no and the form is publicly available, please provide a link in the text box.	[Text Box]
1b. If no, has the software producer submitted a Common Form to the HUD SCRM Program Team?	[Yes/No]
2. Did the organization attest to all of the practices identified in the self-attestation form? If no, please complete subsections a, b, and c.	[Yes/No]
2a. Please list practices unable to be attested to.	[Text Box]
2b. Please detail mitigation practices in place to reduce associated risks.	[Text Box]
2c. Please provide a Plan of Action and Milestones (POA&M) to address these risks.	[Text Box]

5. Services, Assets, or Other Inputs Supplied by Company (check all boxes that apply)

Complete each of the questions within Tables 5-9 to allow HUD to better understand your company's supply chain risk posture.

Note: HUD may request additional information in support of responses to the following questions.

Note: If needed, additional services may be added to this list by contacting HUD when the solicitation request is available.

1. Please select all services, assets, or other inputs your company will be supplying to HUD.
   - ☒ *Employee Services (e.g., Medical, Training)*
   - ☐ *Research / Data Services (e.g., Housing Research, Data Analytics)*
   - ☐ *Financial Services (e.g., Appraisals, Asset Recovery, Mortgage Accounting, Loan Services)*
   - ☐ *Construction / Property Management (e.g., Plumbing, Property Cleaning, Document Destruction)*
   - ☐ *Information Technology Services (e.g., Telecommunications, Cybersecurity)*
   - ☐ *Information Technology Assets (e.g., IT Software [Microsoft Office] and Hardware [Cisco Routers])*
   - ☐ *Other:*

     [Text Box here for other input]

2. If you selected any of the services in which you would need access to HUD data (e.g., Personnel Data, HUD Customer Data, HUD Program Data), please answer the remaining questions in Section 5.

2a. Provide a brief description of the data that you may need access to.	[Text Box]

2b. Do you have policies and procedures to ensure the confidentiality and integrity of HUD data that you would access?	[Yes/No]
3. Will any HUD data be stored on your network?	[Yes/No]
3a. If yes, how will the data be stored, transmitted, and secured?	[Text Box]
3b. If yes, what is the expected volume of data that will be accessed or stored?	[Text Box]
4. Do you expect to share HUD data with any of your third-party vendors that you will include in engagements with HUD?	[Yes/No]
4a. If yes, which vendors will have access to HUD data?	[Text Box]
4b. If yes, what policies and procedures do you have in place to protect the confidentiality and security of HUD data?	[Text Box]
5. Where will HUD data be stored? *Note: All HUD data is required to be stored within the United States.*	[Text Box]

6. Supply Chain Management and Supplier Governance	
1. Do you have written Supply Chain Risk Management (SCRM) requirements in your contracts with your suppliers?	[Yes/No]
1a. How do you verify that your suppliers are meeting contractual terms and conditions, which may include requirements to be passed down to subcontractors?	[Text Box]
1b. If violations of contractual SCRM requirements or SCRM-related incidents occur, do you monitor and track remediation activities to completion?	[Yes/No]
o If yes, briefly describe your remediation procedures.	[Text Box]
2. How often do you review and update your SCRM requirements?	[Drop down with time periods]
3. Do you have a policy or process to ensure that none of your suppliers or third-party components are on any banned list (e.g., ITAR, NDAA Section 889)?	[Yes/No]
3a. If yes, indicate agreement with the following statement. ☐ [Company Name] has processes to review its suppliers and third-party components **AND** is not, to its knowledge, using any products that are on any banned list.	

4. Do you have strategies within your procurement process to verify the integrity of the products, software, or hardware you receive?	[Yes/No]
4a. Do you employ trusted platform modules to verify authenticity of procured hardware or software?	[Yes/No]
4b. Have you had any risk or issues from a counterfeit artifact procured in the last 12-24 months?	[Yes/No]
5. Do you have a process to assess the current security posture subcontractors before hiring them? Note: This also includes assessing the subcontractors' supply chain.	[Yes/No]
6. Do you have policies for your suppliers to notify you when there are changes to their subcontractors or their offerings (components, products, services, or support activities)?	[Yes/No]
Supply Chain Resilience	
7. Does your organization have a formal process for ensuring supply chain resilience as part of your product offering SCRM practices?	[Yes/No]
8. Do you require and audit key suppliers for their ability to be prepared for unexpected supply chain disruptions?	[Yes/No]
9. Does your company consider supplier diversity to avoid single sources and to reduce the occurrence of suppliers being susceptible to the same threats to resilience?	[Yes/No]
10. Does your company consider alternate offering delivery channels to mitigate extended supplier outages to include cloud, network, telecommunication, transportation, and packaging?	[Yes/No]
11. Does your organization conduct contingency planning exercises related to supply chain activities?	[Yes/No]
12. Does your company perform supplier continuous monitor of supply chain risks or services offered to the agency?	[Yes/No]

7. Information Security	
1. Do you follow operational standards or frameworks for managing Information Security/Cybersecurity? (e.g., NIST CSF 1.1, NIST 800-37, Rev. 2, NIST SP 800-161, ISO IEC 27001, ISO 20243, ISO 27036, SAE AS649) Note: These are required to operate at the Federal Government level.	[Yes/No]

1a. If yes, please list the operational standards, frameworks you follow and certifications you have.	[Text Box]
2. Do you have published and publicly available privacy policies?	[Yes/No]
Identify	
3. Do you have a policy or procedure in place to ensure security classifications are considered when handling sensitive information?	[Yes/No]
3a. What is your process to verify that information is classified according to legal, regulatory, or internal sensitivity requirements?	[Text Box]
3b. What are the requirements for data retention, destruction, and encryption?"	[Text Box]
Protect	
4. Do you follow an industry standard or framework for your internal or third-party cloud deployments, if applicable?	[Yes/No]
4a. If yes, please name the industry standard or framework.	[Text Box]
5. Does the functional integrity of your product or services rely on cloud services?	[Yes/No]
5a. If yes, what type of cloud service do you use? (e.g., commercial, public, or hybrid)?	[Text Box]
5b. What policies and procedures are in place to protect the integrity of the data provided through cloud services?	[Text Box]
5c. Where are these data centers located?	[Text Box]
5d. What security controls does your company have in place to ensure HUD data does not leave secure data storage within the United States?	[Text Box]
6. Do you include contractual obligations to protect information and information systems handled by your suppliers?	[Yes/No]
7. Do you have an organizational policy on the use of encryption that conforms with industry standards or control frameworks? Government standard is encryption has to be compliant with FIPS 140-2/140-3	[Yes/No]
7a. What is your process for protecting data at rest and in transit?	[Text Box]
8. What cybersecurity training is required for your third-party stakeholders (e.g., suppliers, customers, partners, etc.) who	[Text Box]

have network access?	
8a. How is training compliance tracked for third parties with network access?	[Text Box]
9. Is cybersecurity training required for personnel who have administrative rights to your enterprise computing resources?	[Yes/No]
9a. What is the frequency for verifying personnel training compliance?	[Text Box]
Detect	
10. Does your incident response plan include methods for detecting incidents in a timely manner to reduce the overall impact?	[Yes/No]
10a. Are cybersecurity events centrally logged, tracked, and continuously monitored?	[Yes/No]
10b. Are incident detection practices continuously improved?	[Yes/No]
11. Do you have a process in place for reporting data breaches that is in compliance with State and Federal requirements?	[Yes/No]
12. Have you had any reports of a security breach or fraudulent activity in the past 3 years?	[Yes/No]
12a. If yes, what measures have you taken to prevent future incidents? If there were multiple reports, please list measures taken for each incident.	[Text Box]
Respond and Recover	
13. Do you have a documented incident response process and a dedicated incident response team (CSIRT - Computer Security Incident Response Team)?	[Yes/No]
14. Does your company have a point of contact for cybersecurity related issues? If yes, please list name and contact details.	[Yes/No] [Text Box]
15. Do you insure for financial harm from a major cybersecurity incident (e.g., self-insure, third-party, parent company, etc.)?	[Yes/No]
15a. Does coverage include financial harm to your customers resulting from a cybersecurity breach which has impacted your company?	[Yes/No]
15b. If yes, what policies and procedures do you have in place to protect the confidentiality and security of HUD data?	[Text Box]

8. Physical Security	
1. Do you have documented security policies and procedures that address the control of physical access to cyber assets (network devices, data facilities, patch panels, industrial control systems, programmable logic, etc.)?	[Yes/No]
2. Are any of the following located outside of the United States? If yes, please provide the country where they are located.	[Yes/No]
Headquarters or Corporate Office	[Text Box]
Operations Center Locations	[Text Box]
Data Centers	[Text Box]
24/7 Security Operations Centers	[Text Box]

9. Personnel Security	
Onboarding and Offboarding	
1. Do you have policies for conducting background checks, as permitted by the country in which you operate, for the following personnel?	
Employees	[Yes/No]
Contractors	[Yes/No]
Suppliers	[Yes/No]
2. Do you have a process for offboarding personnel?	[Yes/No]
Awareness and Training	
3. Are you aware of security training practices performed by your subcontractors to their personnel?	[Yes/No]
4. Are all personnel trained in security best practices? This includes, but is not limited to, supply chain risks and threats, insider threats, access control, and data protection.	[Yes/No]
5. Do you have a Code of Conduct for your employees, suppliers, and subcontractors?	[Yes/No]

10. Signature Block	
Please complete the signature block below to certify the information provided in this questionnaire is accurate and up to date.	
Vendor Representative Full Name:	Role:

Signature:	Date:

----------**End of Survey**----------