a currently approved information collection. In accordance with the requirements of the Paperwork Reduction Act of 1995, this notice seeks comments concerning information required by FEMA to revise National Flood Insurance Program Maps.

DATES: Comments must be submitted on or before December 26, 2023.

ADDRESSES: To avoid duplicate submissions to the docket, please submit comments at *www.regulations.gov* under Docket ID FEMA–2023–0029. Follow the instructions for submitting comments.

All submissions received must include the agency name and Docket ID. Regardless of the method used to submitting comments or material, all submissions will be posted, without change, to the Federal eRulemaking Portal at *http://www.regulations.gov,* and will include any personal information you provide. Therefore, submitting this information makes it public. You may wish to read the Privacy and Security Notice that is available via a link on the homepage of *www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Brian Koper, Emergency Management Specialist, Engineering Services Branch, Risk Management Directorate, DHS/FEMA, at *Brian.Koper@fema.dhs.gov* or 202–733–7859. You may contact the Information Management Division for copies of the proposed collection of information at email address: *FEMA-Information-Collections-Management@fema.dhs.gov.*

SUPPLEMENTARY INFORMATION: The National Flood Insurance Program (NFIP) is authorized by the National Flood Insurance Act of 1968, as amended, 42 U.S.C. 4001 *et seq.* The Federal Emergency Management Agency (FEMA) administers the NFIP and maintains the maps that depict flood hazard information. Communities are required to submit technical information concerning flood hazards and plans to avoid potential flood hazards when physical changes occur (*see* 44 CFR 65.3). Communities are provided the right to submit technical information when inconsistencies on maps are identified (*see* 44 CFR 65.4). In order to revise the Base (one-percent annual chance) Flood Elevations (BFEs), Special Flood Hazard Areas (SFHAs), and floodways presented on the NFIP maps, a community must submit scientific or technical data demonstrating the need for a revision. The NFIP regulations outline the data that must be submitted for these requests (*see* 44 CFR part 65). This collection serves to provide a standard format for the general information requirements outlined in the NFIP regulations and helps establish an organized package of the data needed to revise NFIP maps.

Collection of Information

Title: Revision to National Flood Insurance Program Maps: Application Forms for LOMRs and CLOMRs.

Type of Information Collection: Renewal of a currently approved information collection.

OMB Number: 1660–0016.

FEMA Forms: FEMA Form FF–206–FY–21–100 (formerly 086–0–27), Overview & Concurrence (Form 1); FEMA Form FF–206–FY–21–101 (formerly 086–0–27A), Riverine Hydrology & Hydraulics (Form 2); FEMA Form FF–206–FY–21–102 (formerly 086–0–27B), Riverine Structures (Form 3); FEMA Form FF–206–FY–21–103 (formerly 086–0–27C), Coastal Analysis (Form 4); FEMA Form FF–206–FY–21–104 (formerly 086–0–27D), Coastal Structures (Form 5); and FEMA Form FF–206–FY–21–105 (formerly 086–0–27E), Alluvial Fan Flooding (Form 6).

Abstract: The forms in this information collection are used to determine if the collected data will result in the modification of Base Flood Elevations (BFEs), Special Flood Hazard Area (SFHA), or floodway. Once the information is collected, it is submitted to FEMA for review and is subsequently included on the National Flood Insurance Program (NFIP) maps. These maps will be used for flood insurance determinations and for floodplain management purposes.

Affected Public: State, Local and Tribal Government, Business or Other For-Profit, Individuals or Households.

Estimated Number of Respondents: 5,589.

Estimated Number of Responses: 5,589.

Estimated Total Annual Burden Hours: 14,633.

Estimated Total Annual Respondent Cost: $1,082,824.

Estimated Respondents' Operation and Maintenance Costs: $26,430,000.

Estimated Respondents' Capital and Start-Up Costs: $0.

Estimated Total Annual Cost to the Federal Government: $26,240.

Comments

Comments may be submitted as indicated in the **ADDRESSES** caption above. Comments are solicited to (a) evaluate whether the proposed data collection is necessary for the proper performance of the Agency, including whether the information shall have practical utility; evaluate the accuracy of the Agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (c) enhance the quality, utility, and clarity of the information to be collected; and (d) minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submission of responses.

Millicent Brown Wilson,

Records Management Branch Chief, Office of the Chief Administrative Officer, Mission Support, Federal Emergency Management Agency, Department of Homeland Security.

[FR Doc. 2023–23667 Filed 10–25–23; 8:45 am]

BILLING CODE 9110–12–P

DEPARTMENT OF HOMELAND SECURITY

[CISA–2023–0026]

Request for Comment on Software Identification Ecosystem Option Analysis

AGENCY: Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

ACTION: Notice; request for information.

SUMMARY: The Cybersecurity and Infrastructure Security Agency (CISA) announces the publication of ''Software Identification Ecosystem Option Analysis,'' which is a white paper on software identification ecosystems and requests public comment on the paths forward identified by the paper and on the analysis of the merits and challenges of the software identifier ecosystems discussed. Additionally, CISA requests input on analysis or approaches currently absent from the paper.

DATES: Written comments are requested on or before December 11, 2023. Submissions received after that date may not be considered.

ADDRESSES: You may send comments, identified by CISA–2023–0026, by any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for sending comments.

Instructions: All submissions received must include the words ''Cybersecurity and Infrastructure Security Agency'' and the docket number for this action. Comments received will be posted without alteration at *http://*

www.regulations.gov, including any personal information provided.

Docket: For access to the docket and comments received, please go to *www.regulations.gov* and enter docket number CISA–2023–0026.

To submit comments electronically:

1. Go to *www.regulations.gov,* and enter CISA–2023–0026 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. Do not include personal information, such as account numbers or Social Security numbers, or names of other individuals. 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.

Commenters may access the ''Software Identification Ecosystem Option Analysis'' white paper on CISA's website at: *https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis.*

FOR FURTHER INFORMATION CONTACT: Allan Friedman, 202–961–4349, *sbom@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION:

I. Public Participation

Interested persons are invited to comment on this notice by submitting written data, views, or arguments using the method identified in the **ADDRESSES** section. All members of the public, including, but not limited to, specialists in the field, academic experts, industry, public interest groups, and those with relevant economic expertise, are invited to comment.

II. Background

Software identification is a key facilitator of effective vulnerability management. Software identifiers are labels for specific versions of software that conform to a defined format. An identifier enables users to track software in relation to other information, such as known vulnerabilities, mitigations for vulnerabilities, lists of approved or disallowed software, and adversary activities. An effective, harmonized software identification ecosystem will facilitate greater automation, inventory visibility, and broader, more effective use of software bills of materials (SBOMs).

The two key requirements for an effective software identification ecosystem are:

1. Timely availability of software identifiers across all software items; and
2. Software identifiers that support both precise identification and grouping of software items.

Key challenges for an effective software identification ecosystem are: (1) uniformly and deterministically generating or locating the identifier for an unknown piece of software (discoverability); (2) distributing unique identifiers for software such that one identifier is not associated with multiple software or versions (precision); and (3) developing a mechanism by which software versions are associated with each other (grouping).

The white paper evaluates the following key criteria for a successful software identifier format:

1. Identifiers all refer to a single variant of a given piece of software and support grouping expressions.
2. Identifiers are built to express a fine level of granularity with support for complete identifier enumeration.

Three software identifier formats are starting points, based on their current use and future potential:

Common Platform Enumeration (CPE): In a system based on CPE, a set of parties generate the software identifiers for the community. Each identifier is generated at a point in time and then distributed to the community.

Package URLs (purl): In a system based on purl, any number of parties may generate software identifiers for the community. purl's existing mechanisms for distributed identification generation also make it feasible as the foundation for a system with a searchable database, however its lack of uniformity presents challenges.

OmniBOR: In a system built on OmniBOR, any party is able to derive a software's identifier from an instance of a piece of software. These identifiers are mechanically generated based on inherent properties of a piece of software, which are available to anyone who has that piece of software. In some cases, these identifiers also contain information about the composition of the software, enabling further identification of its components.

The white paper identifies six paths forward for a software identification ecosystem. Although the paths are individually evaluated, they are not mutually exclusive as a solution.

1. Any party can generate a software's identifier. Inherent identifiers are used.
2. Many parties generate software identifiers. The generators then push the software identifiers to the community through the distribution of the software. Defined software identifiers are used.
3. A central authority oversees and supports the many parties who generate and distribute software identifiers. Defined software identifiers are used.
4. An active management system other than a central authority oversees and supports the many parties that generate inherent identifiers. Defined identifiers are used.
5. In addition to a defined identifier scheme (Paths 2, 3, and 4) there is a standardized structure to characterize unknown software. Correlation is done using fuzzy-matching over the set of provided characteristics.
6. Many parties use multiple defined identifier formats to generate software identifiers.

The ''Software Identification Ecosystem Option Analysis'' white paper identifies paths forward in solving the problem of software identification and explores the benefits and challenges of the various approaches, as well as the community or authority structure that would be needed to develop and sustain the identifier format ecosystem. In doing so, the white paper outlines the requirements and activities necessary to establish a harmonized software identification ecosystem to facilitate greater automation, inventory visibility, and the multi-faceted value proposition of broad adoption of Software Bill of Materials (SBOM).

III. List of Topics for Commenters

Commenters may access the ''Software Identification Ecosystem Option Analysis'' white paper on CISA's website at: *https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis.* CISA seeks comments on the following topics:

(1) Key requirements for an effective software identification ecosystem
(2) Merits and challenges of available software identifier formats
(3) The viability of a system reliant on inherent identifiers or defined identifiers
(4) The necessity of a central authority or other active managing body for a software identifier ecosystem
(5) Methodology for division of software identification responsibilities in an ecosystem where multiple software identifier formats are used
(6) Preferred paths forward

(7) Issues, challenges, or use cases not considered or addressed in the paper

(8) Stakeholders that should be included in deliberation

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

Eric Goldstein,

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

[FR Doc. 2023–23668 Filed 10–25–23; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

FY 2023 Senior Executive Service Performance Review Boards

AGENCY: Department of Homeland Security.

ACTION: Notice.

SUMMARY: This notice announces the appointment of members of the FY 2023 Senior Executive Service (SES) Performance Review Boards (PRBs) for the Department of Homeland Security (DHS). The purpose of the PRBs is to make recommendations to the appointing authority (*i.e.,* Component Head) on the performance of senior executives (career, noncareer, and limited appointees), including recommendation on performance ratings, performance-based pay adjustments, and performance awards. The PRBs will also make recommendations on the performance of Transportation Security Executive Service, Senior Level, and Scientific and Professional employees. To make its recommendations, the PRBs will review performance appraisals, initial summary ratings, any response by the employee, and any higher-level official's recommendation.

DATES: This Notice is applicable as of October 26, 2023.

FOR FURTHER INFORMATION CONTACT: Christian Fajardo, Human Resources Specialist, Office of the Chief Human Capital Officer, *christian.fajardo@hq.dhs.gov,* 771–200–0392.

SUPPLEMENTARY INFORMATION: In accordance with 5 U.S.C. 4314(c) and 5 CFR 430.311, each agency must establish one or more PRBs to make recommendations to the appointing authority (*i.e.,* Component Head) on the performance of its senior executives. Each PRB must consist of three or more members. More than one-half of the membership of a PRB must be SES career appointees when reviewing appraisals and recommending performance-based pay adjustments or performance awards for career appointees. Composition of the specific PRBs will be determined on an ad hoc basis from among the individuals listed below:

List of Names (Alphabetical Order)

Abdelall, Brenda
Acosta, Juan L
Adamcik, Carol A
Aguilar, Max
Anguilar, Raul
Alfonso-Royals, Angelica
Alles, Randolph D
Almeida, Corina
Anderson, Sandra D
Antalis, Casie
Antognoli, Anthony
Armstrong, Gloria R
Arratia, Juan
Arvelo, Ivan J
Baidwan, Hemant S
Baker, Jeremy D
Baker, Paul E
Barksdale-Perry, Nicole C
Baroukh, Nader
Barrera, Staci A
Basham, Craig
Beattie, Brien
Belcher, Brian C
Berg, Peter B
Berger, Katrina W
Bhagowalia, Sanjeev
Bible, Daniel A
Bible, Kenneth
Blackwell, Juliana J
Bobich, Jeffrey M
Borka, Robert
Boulden, Laurie
Boyd, John
Brane, Michelle
Braun, Jacob H
Breitzke, Erik P
Brewer, Julie S
Bright, Andrea J
Brito, Roberto
Brown, Allen S
Brown, Roger
Browne, Rene E
Brundage, Christopher
Brundage, William
Bryson, Tony
Bucholtz, Kathleen L
Buetow, Zephranie
Bullock, Edna
Burgess, Kenneth
Burks, Atisha
Burriesci, Kelli A
Burrola, Francisco
Bush, William B
Cagen, Steven W
Caine, Jeffrey
Callahan, Mary Ellen
Cameron, Michael K
Canevari, Holly E
Cantu, John
Canty, Rachel E
Cappello, Elizabeth A
Carabin, David
Carnes, Alexandra
Carpio, Philip F
Carraway, Melvin J
Chaleki, Thomas D
Charles, Marcos
Cheatle, Kimberly A
Cheng, Wen-Ting
Clark, Alaina
Clark, Kenneth N
Cleary, Jennifer S
Cline, Richard K
Cloe, David
Clutter, Mason
Cofield, Valerie
Companion, Tod T
Condon, John
Cook, Charles
Cooper, Ntina K
Corle, Ryan
Corrado, Janene M
Cotter, Daniel
Courey, Marc B
Courtney, Paul
Cox, Adam
Cox, Debra S
Cross, Catherine C
Crumpacker, Jim H
Cullen-Dunbar, Susan
Cummings, Melanie
Cunningham, John D
Dainton, Albert J
Dargan, John L
Das, Sharmistha
Davidson, Andrew
Davidson, Johnathan
Davidson, Michael J
Dawson, Inga I
Dawson, Mark
De La O, Jennifer B
Deloatch, Reshea
Dembling, Ross W
DeMella, Jill
DeNayer, Larry C
DiFalco, Frank J
Dobitsch, Stephanie M
Doherty, Stephanie
Donahue, James L
Doran, Thomas J
Dorr, Robert
Doyle, Kerry
Dragani, Nancy J
Dunlap, James
Durst, Casey O
Ederheimer, Joshua A
Edwards, B. Roland
Ellison, Jennifer
Emrich, Matthew D
Enriquez Mcdivitt, Myriam
Escobar Carrillo, Felicia A
Espinosa, Marsha
Evetts, Mark V
Feder, Steven
Fenton, Jennifer M
Ferraro, Nina M
Fitzmaurice, Stacey D
Fitzpatrick, Ronnyka
Fluty, Larry D
Fong, Heather
Franklin, Tami K
Fujimura, Paul
Gabbrielli, Tina
Gaches, Michael
Gantt, Kenneth D
Garcia, Bobby
Gersten, David
Giles, Thomas
Gladwell, Angela R
Glass, Veronica M
Gorman, Chad M
Gountanis, John
Granger, Christopher