rainfall, changing weather patterns, riverine and coastal erosion, and shifts in future development.

- Particularly where comments relate to the CRS program's costs or benefits, comments will be most useful if there are data and experience under the program available to ascertain the program's actual impact.

C. List of Questions for Commenters

The below non-exhaustive list of questions is meant to assist members of the public in the formulation of comments and is not intended to restrict the issues that commenters may address:

(1) What are the strengths of the current CRS program? What components of the program are currently working well and why?

(2) What are the challenges with the current CRS program that need to be addressed and why? How can the CRS program be modified, expanded, or streamlined to better address or resolve these challenges?

(3) While the CRS program is technically available to all compliant NFIP communities, is access to the CRS program equitable for all communities? If not, what changes to the CRS program could make it more equitable for all communities? How could the CRS program provide better outreach to disadvantaged communities to encourage participation? How could the CRS program provide better outreach to households in disadvantaged communities to encourage participation in the NFIP?

(4) How could the CRS program better promote and/or incentivize improved reduction of future conditions and risks such as climate change, sea-level rise, urban flooding, and future development?

(5) How could the CRS program better address the mitigation of repetitive loss/severe repetitive loss [14] properties and how could FEMA further leverage the CRS program to achieve mitigation of repetitive loss/severe repetitive loss properties?

(6) How can the CRS program be modified, expanded, or streamlined to best incentivize participation by communities and flood insurance policyholders to become more resilient and lower their vulnerability to flood risk?

(7) How can the CRS program better incentivize floodplain management, risk management, and/or risk reduction efforts for communities through CRS discounts, grants, trainings, technical assistance or other means? Which efforts are most critical for the CRS program to support?

(8) What existing sources of data can FEMA leverage to better assist communities to assess, communicate, and drive the reduction of current and future flood risk? Can FEMA leverage new technologies to modify or streamline the CRS program? If so, what are they and how can FEMA use new technologies to achieve the statutory objectives of the program?

(9) The CRS program provides credits for flood risk reduction activities. Are there flood risk reduction activities that are not currently given credit within the CRS program that should be? If so, what are they and why? Are there flood risk reduction activities that are currently given excessive credit within the CRS program than they should be given? If so, what are they and why? Should the CRS program provide a list of optional risk reduction activities for communities to choose from or a list of required risk reduction activities, and why?

(10) What successful approaches have been taken by State, local, Tribal, and Territorial governments that the CRS program could leverage to better support community participation in the CRS program? In what ways could the CRS program better support States, Tribes, Territories and Regions, and flood control and water management districts to improve community participation in the program? What innovative changes could the CRS program make to be simpler for communities to join and maintain participation?

(11) How could the CRS program provide better outreach to disadvantaged communities to encourage participation? How could the CRS program provide better outreach to households in disadvantaged communities to encourage participation in the NFIP?

(11) In what ways could the CRS program facilitate collaboration across jurisdictional boundaries to support a community's ability to reduce flood risk? How could the CRS program be modified, expanded, or streamlined to allow for multi-jurisdictional collaboration efforts to receive credit under the CRS program?

(12) What opportunities exist for the CRS program to better integrate with other entities and/or programs? For example, in what specific ways could the CRS program better work and integrate with State, local, Tribal, and Territorial programs, including but not limited to, floodplain management, emergency services, land use planning and building code administration capital improvement, transportation, redevelopment, pre- and post-disaster recovery, climate adaptation, hazard mitigation planning, watershed management, and/or wetlands, riparian, or environmental management programs? In what specific ways could the CRS program better work and integrate with Federal disaster assistance programs or Federal mitigation programs?

FEMA notes that this notice is issued solely for information and program-planning purposes. Responses to this notice do not bind FEMA to any further actions related to the response.

Deanne Criswell,

Administrator, Federal Emergency Management Agency.

[FR Doc. 2021–18167 Filed 8–20–21; 8:45 am]

BILLING CODE 9111–47–P

[14] ''Repetitive loss properties'' are those properties for which two or more claims of more than $1,000 have been paid by the NFIP within any 10-year period since 1978. ''Severe repetitive loss properties'' are those as defined in the Flood Insurance Reform Act of 2004 that are one-four family properties that have had four or more claims of more than $5,000 or two to three claims that cumulatively exceed the building's value. CRS considers non-residential buildings that also meet these criteria to be severe repetitive loss properties. *See* National Flood Insurance Program Community Rating System Coordinator's Manual 2017 and National Flood Insurance Program Community Rating System Addendum to the 2017 CRS Coordinator's Manual at *https://www.fema.gov/floodplain-management/community-rating-system* (last accessed May 20, 2021).

DEPARTMENT OF HOMELAND SECURITY

[Docket Number DHS–2021–0009]

Agency Information Collection Activities: Vulnerability Discovery Program, 1601–0028

AGENCY: Department of Homeland Security, (DHS).

ACTION: 30-Day notice and request for comments; extension without change of a currently approved collection, 1601–0028.

SUMMARY: The Department of Homeland Security, will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995. DHS previously published this information collection request (ICR) in the **Federal Register** on Friday, March 19, 2021 for a 60-day public comment period. There were three public comments received by DHS. The purpose of this notice is to allow additional 30-days for public comments.

DATES: Comments are encouraged and will be accepted until September 22, 2021. This process is conducted in accordance with 5 CFR 1320.1

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/PRAMain.* Find this particular information collection by selecting ''Currently under 30-day Review—Open for Public Comments'' or by using the search function.

SUPPLEMENTARY INFORMATION: Security vulnerabilities, defined in section 102(17) of the Cybersecurity Information Sharing Act of 2015, are any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control. Security vulnerability mitigation is a process starting with discovery of the vulnerability leading to applying some solution to resolve the vulnerability. There is constantly a search for security vulnerabilities within information systems, from individuals or nation states wishing to bypass security controls to gain invaluable information, to researchers seeking knowledge in the field of cyber security. Bypassing such security controls in the DHS and other Federal Agencies information systems can cause catastrophic damage including but not limited to loss in Personally Identifiable Information (PII), sensitive information gathering, and data manipulation.

Pursuant to section 101 of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, (commonly known as the SECURE Technologies Act) individuals, organizations, and/or companies may submit any discovered security vulnerabilities found associated with the information system of any Federal agency. This collection would be used by these individuals, organizations, and/or companies who choose to submit a discovered vulnerability found associated with the information system of any Federal agency.

Specifically, DHS and Federal cybersecurity agencies are working to address the recently discovered SolarWinds hack on Federal agencies and organizations around the world. While DHS had previously obtained approval to collect this information on its own behalf, recent cyber attacks exploiting vulnerabilities have exemplified the need to have this capability government-wide. In 2020, a major cyberattack, nicknamed the SolarWinds cyberattack, by a group backed by a foreign government penetrated thousands of organizations globally including multiple parts of the United States federal government, leading to a series of data breaches. The cyberattack and data breach were reported to be among the worst cyber-espionage incidents ever suffered by the U.S., due to the sensitivity and high profile of the targets and the long duration (eight to nine months) in which the hackers had access. Affected organizations worldwide included NATO, the U.K. government, the European Parliament, Microsoft and others.

Public Law 116–283, Sec. 1705 (which amended 44 U.S.C. 3553) permits extensive sharing of information regarding cybersecurity and the protection of information and information systems from cybersecurity risks between Federal Agencies covered by the Federal Information Security Modernization Act and the Department of Homeland Security. This unique authority makes DHS well positioned to host the approval of this information collection on behalf of other Federal agencies.

DHS is requesting pursuant to 44 US Code 3509, that the information collection be designated for any Federal agencies ability to utilize the standardized DHS online form to collect their own agency's vulnerability information and post the information on their own agency websites.

The form will include the following essential information:

- Vulnerable host(s)
- Necessary information for reproducing the security vulnerability
- Remediation or suggestions for remediation of the vulnerability
- Potential impact on host, if not remediated

This form will allow Federal agencies to complete the following actions; (1) allow the individuals, organizations, and/or companies who discover vulnerabilities in the information systems to report their findings to the agency, and (2) provide the agencies initial insight into any newly discovered vulnerabilities, as well as zero-day vulnerabilities in order to mitigate the security issues prior to malicious actors acting upon the vulnerability for malicious intent.

The form will also benefit researchers and will provide a safe and lawful method to practice and discover new cyber methods to discover the vulnerabilities. It will provide the same benefit to Federal agencies and will promote the enhancement of Federal information system security policies.

Respondents will be able to submit their information directly to the agency in which they would like to report a vulnerability. Federal Agencies will provide the form electronically via their agencies website.

The information collected does not have an impact on small business or other small entities.

The collection of this information related to the discovery of security vulnerabilities by individuals, organizations, and/or companies is needed to fulfill the congressional mandate in Section 101 of the SECURE Technologies Act related to creating Vulnerability Disclosure Policies. In addition, without the ability to collect information on newly discovered security vulnerabilities associated with Federal agency information systems, Federal agencies will rely solely on the internal security personnel and/or the discovery through a post occurrence breach of security controls.

There are no assurances of confidentiality provide. Any PII that is collected will be for the sole purpose of feedback and dialogue. Federal Agencies will ensure the collection of information is covered by a Systems of Record Notice and will display a Privacy Notice to the respondents.

There are no changes to the information being collected.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

2. 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;

3. Enhance the quality, utility, and clarity of the information to be collected; and

4. 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 submissions of responses.

Analysis

Agency: Department of Homeland Security, (DHS).

Title: Vulnerability Discovery Program.

OMB Number: 1601–0028.

Frequency: On Occasion.

Affected Public: State, Local and Tribal Government.

Number of Respondents: 3,000.

Estimated Time per Respondent: 1 Hour.

Total Burden Hours: 3,000.

Robert Dorr,

Executive Director, Business Management Directorate.

[FR Doc. 2021–18059 Filed 8–20–21; 8:45 am]

BILLING CODE P

DEPARTMENT OF HOMELAND SECURITY

[Docket Number DHS–2021–0027]

Agency Information Collection Activities: DHS Civil Rights and Civil Liberties Complaint and Privacy Waiver Form

AGENCY: Department of Homeland Security (DHS).

ACTION: 30-Day notice and request for comments.

SUMMARY: The Department of Homeland Security, will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted until September 22, 2021. This process is conducted in accordance with 5 CFR 1320.1.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/PRAMain.* Find this specific information collection by selecting ''Currently under 30-day Review—Open for Public Comments'' or by using the search function.

SUPPLEMENTARY INFORMATION: The U.S. Department of Homeland Security (DHS), Office for Civil Rights and Civil Liberties (CRCL) reviews and investigates civil rights and civil liberties complaints filed by the public regarding U.S. Department of Homeland Security (DHS) policies and activities. Under 6 U.S.C. 345 and 42 U.S.C. 2000ee–1, CRCL reviews and assesses allegations involving a range of alleged civil rights and civil liberties abuses, such as:

- Discrimination based on race, ethnicity, national origin, religion, sex, sexual orientation, gender identity, or disability;
- Violation of rights while in immigration detention or as subject of immigration enforcement;
- Discrimination or inappropriate questioning related to entry into the United States;
- Violation of due process rights, such as the right to timely notice of charges or access to lawyer;
- Violation of confidentiality provisions of the Violence Against Women Act;
- Physical abuse or any other type of abuse;
- Denial of meaningful access to DHS or DHS-supported programs, activities, or services due to limited English proficiency and
- Any other civil rights, civil liberties, or human rights violation related to a Department program or activity, including allegations of discrimination by an organization or program that receives financial assistance from DHS.

CRCL also reviews and investigates human rights complaints under Executive Order 13107, disability accommodation complaints under Section 504 of the Rehabilitation Act of 1973, and inaccessible Information and Communication Technology (ICT) complaints under Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (Pub. L. 105–220), codified at 29 U.S.C. 794. The information collected on this form will allow CRCL to review and investigate civil rights and civil liberties complaints filed by the public regarding DHS programs and activities.

CRCL submits copies all external allegations of civil rights and civil liberties violations within its jurisdiction that it receives to the DHS Office of Inspector General (OIG) for review because OIG has the right of first refusal to investigate any allegations. If the OIG declines to investigate the allegations, CRCL may investigate. CRCL coordinates with DHS Components and the OIG regarding matters that CRCL opens as complaint investigations as well as some it decides not to investigate. In general, CRCL shares the incoming information with the Components involved and coordinates with the Components throughout a CRCL investigation. As a result of its complaint investigations, CRCL issues recommendations to DHS Components to address issues of concern and to enhance the agency's civil rights and civil liberties protections. CRCL has also engaged with Components on the implementation of such recommendations.

In addition, the information provided is entered into a CRCL complaint management system (CMS) and may be used by CRCL to track allegations and identify trends and systemic issues that are within CRCL's jurisdiction regardless of whether CRCL investigates an individual allegation. CRCL has used information from these database records to notify DHS Components of issue areas and locations that may warrant closer attention.

Information can be submitted to CRCL via U.S. mail, email, fax, or telephone and may be initiated by members of the public, federal agencies, or agency personnel, non-governmental organizations, media reports or other sources. The use of the complaint form is optional.

The form is in a fillable accessible PDF format and can be submitted by U.S. mail, email, or fax to CRCL. The use of this form provides an efficient means for collecting and processing required data and information useful to conduct an investigation. To minimize administrative burden on complainants and the Department, submission of information electronically, via email, is the fastest way to reach CRCL. Information provided by complainants is maintained in electronic format, so provided the information electronically will further minimize administrative burden.

If a complainant is unable to or does not wish to submit their information electronically, information can be submitted via U.S. mail, fax, or phone call. It is noted on CRCL's website that postal mail can take up to 20 business days. CRCL is about the launch a new CMS that would support other means of submitting a complaint (*e.g.,* web portal) and these are enhancements that will be considered in the future.

This information collection does not have an impact on small businesses or other small entities.

If the information collection is not conducted or is conducted less frequently, CRCL may not be able to effectively fulfill its statutory obligation to the public to review and investigate allegations involving alleged civil rights and civil liberties abuses regarding DHS polices and activities.

Consequences for not using the fillable form include overall delays in processing and an increased frequency in need to follow up with complainants to obtain the types of information requested on the form.

The assurance of confidentiality provided to the respondents for this information collection will be provided by: CRCL's statute under 6 U.S.C. 345, 42 U.S.C. 2000ee–1; the Privacy Impact Assessment for the CRCL Complaint Form and Privacy Waiver; and the Systems of Record Notice: Department of Homeland Security/ALL–029 Civil Rights and Civil Liberties Records