Management Agency, 500 C Street SW, Washington, DC 20472, (202) 646–2833.

SUPPLEMENTARY INFORMATION: Notice is hereby given that, in a letter dated February 14, 2021, the President issued an emergency declaration under the authority of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121–5207 (the Stafford Act), as follows:

I have determined that the emergency conditions in the State of Texas resulting from a severe winter storm beginning on February 11, 2021, and continuing, are of sufficient severity and magnitude to warrant an emergency declaration under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121 *et seq.* (''the Stafford Act''). Therefore, I declare that such an emergency exists in the State of Texas.

You are authorized to provide appropriate assistance for required emergency measures, authorized under Title V of the Stafford Act, to save lives and to protect property and public health and safety, and to lessen or avert the threat of a catastrophe in the designated areas. Specifically, you are authorized to provide assistance for emergency protective measures (Category B) for mass care and sheltering and direct federal assistance under the Public Assistance program.

Consistent with the requirement that federal assistance be supplemental, any federal funds provided under the Stafford Act for Public Assistance will be limited to 75 percent of the total eligible costs. In order to provide federal assistance, you are hereby authorized to allocate from funds available for these purposes such amounts as you find necessary for federal emergency assistance and administrative expenses.

Further, you are authorized to make changes to this declaration for the approved assistance to the extent allowable under the Stafford Act.

The Federal Emergency Management Agency (FEMA) hereby gives notice that pursuant to the authority vested in the Administrator, Department of Homeland Security, under Executive Order 12148, as amended, Jerry S. Thomas, of FEMA is appointed to act as the Federal Coordinating Officer for this declared emergency.

The following areas of the State of Texas have been designated as adversely affected by this declared emergency:

Emergency protective measures (Category B) for mass care and sheltering and direct federal assistance under the Public Assistance program at 75 percent federal funding for all 254 counties in the State of Texas.

The following Catalog of Federal Domestic Assistance Numbers (CFDA) are to be used for reporting and drawing funds: 97.030, Community Disaster Loans; 97.031, Cora Brown Fund; 97.032, Crisis Counseling; 97.033, Disaster Legal Services; 97.034, Disaster Unemployment Assistance (DUA); 97.046, Fire Management Assistance Grant; 97.048, Disaster Housing Assistance to Individuals and Households In Presidentially Declared Disaster Areas; 97.049, Presidentially Declared Disaster Assistance—Disaster Housing Operations for Individuals and Households; 97.050, Presidentially Declared Disaster Assistance to Individuals and Households—Other Needs; 97.036, Disaster Grants—Public Assistance (Presidentially Declared Disasters); 97.039, Hazard Mitigation Grant.

Robert J. Fenton,

Senior Official Performing the Duties of the Administrator, Federal Emergency Management Agency.

[FR Doc. 2021–05792 Filed 3–18–21; 8:45 am]

BILLING CODE 9111–23–P

DEPARTMENT OF HOMELAND SECURITY

Federal Emergency Management Agency

[Internal Agency Docket No. FEMA–4493–DR; Docket ID FEMA–2021–0001]

Puerto Rico; Amendment No. 4 to Notice of a Major Disaster Declaration

AGENCY: Federal Emergency Management Agency, DHS.

ACTION: Notice.

SUMMARY: This notice amends the notice of a major disaster declaration for the Commonwealth of Puerto Rico (FEMA–4493–DR), dated March 27, 2020, and related determinations.

DATES: This change occurred on February 27, 2021.

FOR FURTHER INFORMATION CONTACT: Dean Webster, Office of Response and Recovery, Federal Emergency Management Agency, 500 C Street SW, Washington, DC 20472, (202) 646–2833.

SUPPLEMENTARY INFORMATION: The Federal Emergency Management Agency (FEMA) hereby gives notice that pursuant to the authority vested in the Administrator, under Executive Order 12148, as amended, Thomas J. Fargione, of FEMA is appointed to act as the Federal Coordinating Officer for this disaster.

This action terminates the appointment of David I. Maurstad as Federal Coordinating Officer for this disaster.

The following Catalog of Federal Domestic Assistance Numbers (CFDA) are to be used for reporting and drawing funds: 97.030, Community Disaster Loans; 97.031, Cora Brown Fund; 97.032, Crisis Counseling; 97.033, Disaster Legal Services; 97.034, Disaster Unemployment Assistance (DUA); 97.046, Fire Management Assistance Grant; 97.048, Disaster Housing Assistance to Individuals and Households In Presidentially Declared Disaster Areas; 97.049, Presidentially Declared Disaster Assistance—Disaster Housing Operations for Individuals and Households; 97.050, Presidentially Declared Disaster Assistance to Individuals and Households—Other Needs; 97.036, Disaster Grants—Public Assistance (Presidentially Declared Disasters); 97.039, Hazard Mitigation Grant.

Robert J. Fenton,

Senior Official Performing the Duties of the Administrator, Federal Emergency Management Agency.

[FR Doc. 2021–05804 Filed 3–18–21; 8:45 am]

BILLING CODE 9111–23–P

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: 60-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.

DATES: Comments are encouraged and will be accepted until May 18, 2021. This process is conducted in accordance with 5 CFR 1320.1

ADDRESSES: You may submit comments, identified by docket number Docket # DHS–2021–0009, at:

○ *Federal eRulemaking Portal: http://www.regulations.gov.* Please follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name and docket number Docket # DHS–2021–0009. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to *http://ww.regulations.gov.*

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. 2021–05767 Filed 3–18–21; 8:45 am]

BILLING CODE 9112–FL–P