U.S. Department of Homeland Security
Washington, DC 20528

March 3, 2021

Dominic J. Mancini
Acting Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget
Washington, DC 20503

Dear Mr. Mancini:

This memorandum seeks approval from the Office of Management and Budget (OMB) for a Department of Homeland Security (DHS) emergency approval request under the Paperwork Reduction Act (PRA), 5 CFR 1320.13. The purpose of this ICR is to enable individuals, organizations, and/or companies to submit any vulnerabilities found associated with the information system of any Federal agency. 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 vulnerabilities found associated with the information system of any Federal agency.

The basis for the emergency request under the emergency provisions of the PRA are that the agency cannot reasonably comply with the normal clearance procedures under this part because an unanticipated event has occurred. 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 cyber attack, nicknamed the SolarWinds cyber attack, 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 cyber attack 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.

The attack, which had gone undetected for months, was first publicly reported on December 13, 2020, and was initially only known to have affected the U.S. Treasury Department and the National Telecommunications and Information Administration (NTIA), part of the U.S. Department of Commerce. In the following days, more departments and private organizations reported breaches, including the Department of Homeland Security. The longevity of this hack highlights the need for the Federal Government to partner with well-intentioned cyber security analysts to identify vulnerabilities in the systems of all government agencies.

Pub. L. 116-283, Sec. 1705 (which amended 44 USC 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. While each individual agency will host the sponsored form on their website to collect this information, DHS is proposing to own the approval and notice and comment process for the form on their behalf and on its own. This information will be shared with DHS and other entities in accordance with the agency's individual notices under the Privacy Act of 1974 and all relevant Federal Law.

DHS requests that OMB grant this emergency approval request.

Sincerely,

ERIC N HYSEN

Digitally signed by ERIC N HYSEN
Date: 2021.03.04 08:26:37 -05'00'

Eric Hysen
Chief Information Officer

Enclosures

1601-0028_Vulnerablity Discovery Program _SSA

VDP Form_Questions