U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Chief Information Officer
Washington, DC 20528

December 14, 2023

DECISION

FOR: Richard Revesz
Administrator, Office of Information and Regulatory Affairs,
Office of Management and Budget

THROUGH: Eric Hysen
Chief Information Officer
U.S. Department of Homeland Security

ERIC N HYSEN
Digitally signed by ERIC N HYSEN
Date: 2023.12.19 13:55:43 -05'00'

FROM: Robert J. Costello
Chief Information Officer
Cybersecurity & Infrastruture Security Agency

ROBERT J COSTELLO
Digitally signed by ROBERT J COSTELLO
Date: 2023.12.19 11:35:11 -05'00'

SUBJECT: Request for Emergency Clearance: CISA Gateway User Registration

---

The Cybersecurity & Infrastructure Security Agency requests the Office of Management and Budget (OMB) use the emergency review and approval process to reinstate an expired Paperwork Reduction Act (PRA) information collection, 1670-0009 CISA Gateway User Registration.

Due to an internal workflow failure, which has been remediated, the package expired on August 31, 2023. OMB initially approved the collection on October 9, 2007, and the most recent re-approved it on August 28, 2020, with an expiration date of August 31, 2023. Following the discovery of the workflow failure, the CISA PRA team, with support from legal counsel, conducted an expedited internal review of the package and completed this review on September 28, 2023. The CISA CIO reviewed and approved the 60-day Federal Register Notice on October 4, 2023. DHS published a full renewal package to the Federal Register and is currently in the 60-day comment period until February 5, 2024.

In accordance with the Paperwork Reduction Act (PRA) and the Office of Management and Budget's (OMB) implementing regulations at 5 C.F.R. § 1320.13: (1) this information is necessary to the mission of the Agency, (2) the use of normal clearance procedures is reasonably likely to cause a statutory deadline to be missed. Most importantly, discontinuation of this

collection during the public notice and comment period could result in significant public harm due to the role that this collection plays in the mission performed by CISA in protecting our Nation's critical infrastructure. See below for further explanation regarding (1)– (3).

1. *Essential to the Agency*: The Presidential Policy Directive-21 (PPD-21) (2013) and the National Infrastructure Protection Plan (NIPP) (2013) (Public Law 107-296) highlight the need for a centrally managed repository of infrastructure attributes capable of assessing risks and facilitating data sharing. To support this mission need, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has developed the CISA Gateway. The CISA Gateway contains several capabilities which support the homeland security mission in the area of critical infrastructure (CI) protection. This collection is leveraged by the Critical Infrastructure community, CISA Protective Security Advisors, State Fusion Centers, State, Local, Tribal, and Territorial Governing Coordinating Council (SLTTGCC), Facility owners/operators, and many other government and private partners and sectors. The collection of information uses automated electronic forms. During the online registration process, there is an electronic form used to create a user account and an online training course required to grant access.

2. *The use of normal clearance procedures is reasonably likely to cause a statutory deadline to be missed:* This request for review and approval is vital to continue the mission of the CISA Gateway and support to the Gateway user community. By not collecting this information, the CISA Gateway program is not able to vet and verify a users need to know and cannot not grant access to the system. It is vital that CISA regains this essential capability as soon as possible to support immediate needs in response to delivering and supporting the many SLTT communities that rely on this CISA capability.

3. *Public harm is reasonably likely to result if normal clearance procedures are followed:* This request for review and approval is vital to continue the mission of the CISA Gateway and support to the Gateway user community. Without this information collection, the CISA Gateway program will be unable to vet and verify a user's need to know sensitive information and cannot grant access to the system. The CISA Gateway provides users with some of the most sensitive data available on critical infrastructure, so such an outcome poses a sufficient threat to national security that the system itself might need to be taken offline. This scenario presents a reasonable likelihood that public harm could result. If a potential threat presents itself to CISA, other government agencies, and/or SLTT partners, CISA would not have the ability to provide the Critical Infrastructure data necessary for those private and public partners to effectively respond to a potential threat or event. It is vital that CISA retains this essential capability to support immediate needs in response to delivering and supporting the many SLTT communities that rely on this CISA capability should a Critical Infrastructure event occur to protect the homeland. Since such events can and do occur at random, normal clearance procedures must be stopgrapped by an emergency clearance.

In conclusion, CISA respectfully requests assistance by way of the emergency clearance procedures to ensure the availability of this capability due to critical nature of the collection and the communities being supported by the program. While CISA regrets the now remedied process failure that led to this request and need for assistance, the larger principle of ensuring the security of critical infrastructure for the American public requires immediate action.

Thank you for your time, understanding, and consideration of this request.