to-face discussion or webinar. It is current ULA policy to not accept the ULAT questionnaires in paper format. If there is a power outage at the event site or if the website is down due to technical reasons, facilitators have copies of the paper format for stakeholders to continue filling out. Facilitators do not collect these hard copies. Stakeholders keep them to update the electronic assessment when they next access it.

Technical Assistance Program (TAP) Stakeholder Nomination Form

The TAP Stakeholder Nomination form will be used to assist OBP in the selection of Stakeholders for each Fiscal Year (FY). We take recommendations from IOD personnel and stakeholders to assist in the selection of jurisdictions that will receive OBP Technical Assistance the following FY.

Technical Assistance Stakeholder Feedback Forms

(1) BMAP Stakeholder Feedback Form

Information for this program is being requested to enhance bombing prevention outreach through a voluntary stakeholder feedback form. This stakeholder feedback form would be digital in format and provided to point-of-sale businesses and FSLTT personnel who assist with the program or that have been contacted by BMAP in an effort to spread awareness of suspicious purchasing behavior and suspicious activity related to the acquisition of BMM. This voluntary feedback form would be provided to the point-of-sale business virtually and will only request input based on the experience that the business had with the BMAP team and its ability to conduct outreach. This feedback form will provide vital information which is necessary to streamline and improve processes and will allow BMAP to better target stores that sell BMM moving forward. This feedback form will also allow for an improvement of delivery of BMAP products and provide insight on the jurisdictions that the team visits.

(2) Explosive Blast Modeling (EBM) Stakeholder Feedback Form

The EBM Stakeholder Feedback Form will be used to gauge metrics of the program using the Likert score and assesses OBP annual goals and receives responses regarding actionable recommendations.

(3) Technical Assistance Post Assessment Feedback Form

Information for this program is being requested to assess, re-assess, and validate OBPs Technical Assistance Program pertaining to the delivery of training, products, tools and services to enhance bombing prevention capabilities through a voluntary stakeholder feedback form. This voluntary post assessment feedback form would be digital in format and provided to federal, state, local, tribal, and territorial (FSLTT) stakeholders who have requested OBPs resources through the Technical Assistance Program (TAP). TAP aims to develop and deliver comprehensive preparedness assistance, training, tools, and specialized assistance to a wide variety of stakeholders, to enhance the Nation's security and resiliency against explosive attacks, and to determine specific needs for assistance in managing IED risks and supporting C–IED response. TAP coordinates across OBP and relevant partners to provide communities with to meet their preparedness needs. This voluntary TAP Post Assessment Feedback form would be provided to FSLTT stakeholders virtually and will only request input based on the experience that the FSLTT stakeholders experienced with OBP personnel supporting their communities. This feedback form will provide vital information which is necessary to streamline and improve processes and will allow OBP to better deliver Technical Assistance.

(4) Bomb-Making Awareness Program (BMAP) BOM–D (BMAP Outreach Mobile-Data)) Form

Information for this program is being requested in an effort to enhance bombing prevention outreach throughout the retail community which houses or sells bomb making material (BMM). This information would be collected by Federal State, Local, Tribal, and Territorial (FSLTT) law enforcement personnel and those designated by FSLTT officials to act on their behalf. Information will be used to coordinate efforts with appropriate FSLTT partners who work in the first responder, law enforcement, and bombing prevention realm. Information will be collected by FSLTT partners through electronic methods and will be physically input into this form by FSLTT partners. Information will be collected from business listings located online as well as physical locations identified by FSLTT partners. Information will also be collected by business cards or other means provided to FSLTT partners by businesses who participate.

(5) Explosive Blast Modeling Program (EBM) Request Form

The Explosive Blast Modeling Program Request Form will be used to collect stakeholder location and facility specific information on entities who want the EBM service conducted. This information will be used to contact the stakeholders in order to schedule EBM.

(6) Explosive Detection Canine Handler/Team (EDCT) Needs and Application Survey Form

Providing this EDCT Form to police, fire, corrections, and military entities will enhance the ability of DHS/OBP to accomplish goals related to the DHS Canine and Equine Governance Board while also informing OBP's understanding of the capabilities of the aforementioned entities to provide critical infrastructure security.

This is a new collection (1670–NEW) request.

Analysis

Agency: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

Title: Office for Bombing Prevention Technical Analytics.

OMB Number: 1670–NEW.

Frequency: Annually or less.

Affected Public: Federal, state, local, and tribal government entities, and business or other for-profit.

Number of Respondents: 8,355.

Estimated Time per Respondent: 35 minutes.

Total Burden Hours: 5,057 hours.

Total Burden Cost: $301,337.

Total Annualized Government Cost: $301,337

Winfield P. Werntz,

Acting Chief Information Officer, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

[FR Doc. 2026–10932 Filed 5–29–26; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2026–0001]

Agency Information Collection Activities: .gov Registrar

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)

ACTION: 60-Day notice and request for comments; extension of an existing collection (1670–0049) that was last approved on 10/03/2023 with an expiration date of 10/31/2026.

SUMMARY: The .gov Registry Program within Cybersecurity and Infrastructure Security Agency (CISA) submits the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance.

DATES: Comments are encouraged and will be accepted until *July 31, 2026.*

ADDRESSES: You may submit comments, identified by docket number Docket # CISA–2026–0001, by following the instructions below for submitting comment via the Federal eRulemaking Portal at *https://www.regulations.gov.*

Instructions: All submissions received must include the agency name and docket number Docket # CISA–2026–0001. 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 *https://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Cameron Dixon, 888–282–0870, *help@get.gov.*

SUPPLEMENTARY INFORMATION: .gov is a 'top-level domain' (TLD), similar to .com, .org, or .us. Enterprises use a TLD to register a ''domain name'' (often simply called a domain) for use in their online services, like a website or email. Well-known .gov domains include *whitehouse.gov, congress.gov,* or *uscourts.gov,* but most .gov domains are from non-federal governments like *ny.gov* (State of New York) or *lacounty.gov* (LA County).

.gov is available only to bona fide U.S.-based government organizations and publicly controlled entities. When governments use .gov, they make it harder for would-be impostors to successfully impersonate them online.

Under the DOTGOV Act of 2020 (6 U.S.C. 665), CISA is responsible for the operation and security of the .gov TLD. Pursuant to that law, the .gov program at CISA works to ''provide simple and secure registration of .gov internet domains'', ''ensure that domains are registered and maintained only by authorized individuals'', and ''minimize the risk of .gov internet domains whose names could mislead or confuse users''. In order to provision .gov domains to eligible government entities and ensure adherence to the domain requirements published by CISA pursuant to 6 U.S.C. 665(c), CISA needs to collect information from requestors of .gov domains.

The information will be collected on an online web portal called the ''.gov registrar'', which is built and maintained by CISA. Requestors will be asked to provide information on the characteristics of their government entity (*e.g.,* name, type, physical location, current domain), their preferred .gov domain name (*e.g.,* example.gov), their rationale for the name, organizational contact information (names, phone numbers, email addresses), and nameserver addresses.

Only U.S.-based government organizations are eligible for .gov domains; some of these organizations may be small entities. The collection has been developed to request only the information needed to confirm eligibility and adjudicate a .gov domain request.

Without this collection, CISA will be unable to assess the eligibility of requestors nor provision .gov domains to government organizations. That outcome would decrease cybersecurity for governments across the nation and minimize the public's ability to identify governments online.

In accordance with 6 U.S.C. 665(c)(4), CISA will ''limit the sharing or use of any information'' obtained through this collection ''with any other Department component or any other agency for any purpose other than the administration of the .gov internet domain, the services described in subsection (e), and the requirements for establishing a .gov inventory described in subsection (h).'' Certain metadata for any approved domains (domain name, organization name, nameserver address, city/state information, security contact) will be published online.

This is an extension of an existing collection. Only small, stylistic changes, not substantive updates, have been made since the previous ICR was approved by OMB.

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: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)

Title: .gov registrar.

OMB Number: 1670–0049.

Frequency: Once per domain registered.

Affected Public: Employees representing state, local, territorial, and tribal governments.

Number of Respondents: 3,000 per year.

Estimated Time per Respondent: 20 minutes.

Total Burden Hours: 1,000 hours.

Total Annual Burden Cost: $52,622.

Total Annual Government Burden Cost: $588,600.

Winfield P Werntz,

Acting Chief Information Officer, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2026–10886 Filed 5–29–26; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2026–0067]

Agency Information Collection Activities: State and Local Cybersecurity Grant Program (SLCGP) Evaluation

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: 60-day notice and request for comments; new collection (request for a new OMB Control Number, 1670–NEW).

SUMMARY: The Stakeholder Engagement Division (SED) Grant Analytics Branch within the Cybersecurity and Infrastructure Security Agency (CISA) submits 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 July 31, 2026.

Submissions received after the deadline for receiving comments may not be considered.

ADDRESSES: You may submit comments, identified by docket number Docket #