

State Plan—MHBG.  
 42 U.S.C. 300x-1(b)—Criteria for Plan.  
 42 U.S.C. 300x-1(b)(2)—State Plan for Comprehensive Community Mental Health Services for Certain Individuals—Criteria for Plan—Mental Health System Data and Epidemiology.  
 42 U.S.C. 300x-2(a)—Certain Agreements—Allocations for Systems Integrated Services for Children.  
 Waivers—SUBG.  
 300x-24(b)(5)(B)—Human Immunodeficiency Virus—Requirement regarding Rural Areas.  
 300x-28(d)—Additional Agreements.  
 300x-30(c)—MOE.  
 300x-31(c)—Restrictions on Expenditure of Grant—Waiver Regarding Construction of Facilities.  
 300x-32(c)—Certain Territories.  
 300x-32(e)—Waiver amendment for 1922, 1923, 1924 and 1927.  
 Waivers—MHBG.  
 300x-2(a)(2)—Allocations for Systems Integrated Services for Children.  
 300x-6(b)—Waiver for Certain Territories.  
 Recordkeeping.  
 300x-23—Waiting list.  
 300x-25—Group Homes for Persons in Recovery from Substance Use Disorders.  
 300x-65—Charitable Choice.

TABLE 2—ESTIMATES OF APPLICATION AND REPORTING BURDEN FOR YEAR 2

	Number of respondents	Number of responses per year	Number of hours per response	Total hours
Reporting:				
SUBG .....	60	1	187	11,220
MHBG .....	59	1	187	11,033
Recordkeeping .....	60/59	1	40	2,360
Combined Burden .....				24,613

The total annualized burden for the application and reporting is 33,493 hours (42,373 + 24,613 = 66,986/2 years = 33,493).

Link for the application: <http://www.samhsa.gov/grants/block-grants>.

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](http://www.reginfo.gov/public/do/PRAMain). Find this information collection by selecting “Currently under 30-day Review—Open for Public Comments” or by using the search function.

Alicia Broadus,  
 Public Health Advisor.

[FR Doc. 2023-08337 Filed 4-19-23; 8:45 am]

BILLING CODE 4162-20-P

**DEPARTMENT OF HOMELAND SECURITY**

**Notice of the Renewal of the Critical Infrastructure Partnership Advisory Council Charter**

**AGENCY:** Cybersecurity and Infrastructure Security Agency (CISA), DHS.

**ACTION:** Notice of availability; renewal of the Critical Infrastructure Partnership Advisory Council Charter.

**SUMMARY:** On November 29, 2022, the Secretary of the Department of Homeland Security (DHS) approved the renewal of the Critical Infrastructure Partnership Advisory Council (CIPAC) Charter. Through this notice, the Department is making the renewed CIPAC Charter publicly available and

highlighting updated information and guidelines that have been included in the renewed charter.

**FOR FURTHER INFORMATION CONTACT:**

Amy J. Campbell, 202-372-7014, [amy.campbell@cisa.dhs.gov](mailto:amy.campbell@cisa.dhs.gov).

**SUPPLEMENTARY INFORMATION:** DHS established the CIPAC on March 24, 2006.<sup>1</sup> (71 FR 14930). The Secretary has exempted the CIPAC from the requirements of the Federal Advisory Committee Act (FACA), 5 U.S.C. chapter 10, pursuant to his authority under 6 U.S.C. 451. The CIPAC facilitates interactions between government officials and representatives of owners and/or operators for each of the critical infrastructure sectors established by Presidential Policy Directive 21 and identified in the current National Infrastructure Protection Plan. Please visit <https://www.cisa.gov/critical-infrastructure-partnership-advisory-council> for more information on CIPAC, activities supported by CIPAC, CIPAC Membership Roster, and Council information.

On November 29, 2022, the Secretary of Homeland Security renewed the CIPAC Charter for an additional two years. The renewed CIPAC Charter supersedes the CIPAC Charter dated November 30, 2020, and is available on

<sup>1</sup>The CIPAC was established consistent with 6 U.S.C. 121 and 6 U.S.C. 451(a). Pursuant to the Cybersecurity and Infrastructure Security Agency Act of 2018, the National Protection and Programs Directorate (NPPD) was re-designated as CISA and the authorities related to the CIPAC under 6 U.S.C. 121 were transferred to 6 U.S.C. 652.

the CIPAC website at <https://www.cisa.gov/critical-infrastructure-partnership-advisory-council>. The renewed CIPAC Charter includes new and clarifying information and guidelines concerning: (1) annual training requirements related to ethics standards and information sharing; (2) activities to ensure council membership is able to accomplish mission goals and objectives of the sector; and (3) a provision related to the sharing of classified information.

Dated: April 14, 2023.

Amy J. Campbell,  
 Designated Federal Official, Critical Infrastructure Partnership Advisory Council, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2023-08302 Filed 4-19-23; 8:45 am]

BILLING CODE 9110-9P-P

**DEPARTMENT OF HOMELAND SECURITY**

[Docket No. CISA-2022-0018]

**Request To Revise and Extend the Chemical Security Assessment Tool (CSAT) Information Collection Under the Paperwork Reduction Act**

**AGENCY:** Cybersecurity and Infrastructure Security Agency, DHS.

**ACTION:** 30-Day notice and request for comments.

**SUMMARY:** The Infrastructure Security Division (ISD) within the Cybersecurity and Infrastructure Security Agency

(CISA) 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. CISA previously published this ICR in the **Federal Register** on December 27, 2022, for a 60-day comment period. No comments were received for this ICR during the 60-day public comment period. In this notice, CISA solicits public comment concerning this ICR for an additional 30 days.

**DATES:** Comments are due by May 22, 2023.

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

All submissions received must include the agency name “CISA” and docket number CISA–2022–0018.

Comments that include protected information such as trade secrets, confidential commercial or financial information, Chemical-terrorism Vulnerability Information (CVI),<sup>1</sup> Sensitive Security Information (SSI),<sup>2</sup> or Protected Critical Infrastructure Information (PCII)<sup>3</sup> should not be submitted to the public docket. Comments containing protected information should be appropriately marked and packaged in accordance with all applicable requirements and submission must be coordinated with the point of contact for this notice provided in **FOR FURTHER INFORMATION CONTACT** section.

**FOR FURTHER INFORMATION CONTACT:** Annie Hunziker Boyer, 703–603–5000, [CISARegulations@cisa.dhs.gov](mailto:CISARegulations@cisa.dhs.gov).

**SUPPLEMENTARY INFORMATION:** The CFATS Program identifies chemical facilities of interest and regulates the security of high-risk chemical facilities through a risk-based approach. The CFATS Program is authorized under the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 or “CFATS Act of 2014.”<sup>4</sup>

<sup>1</sup> For more information about CVI see 6 CFR 27.400 and the CVI Procedural Manual at [www.dhs.gov/publication/safeguarding-cvi-manual](http://www.dhs.gov/publication/safeguarding-cvi-manual).

<sup>2</sup> For more information about SSI see 49 CFR part 1520 and the SSI Program web page at [www.tsa.gov/for-industry/sensitive-security-information](http://www.tsa.gov/for-industry/sensitive-security-information).

<sup>3</sup> For more information about PCII see 6 CFR part 29 and the PCII Program web page at [www.dhs.gov/pcii-program](http://www.dhs.gov/pcii-program).

<sup>4</sup> The CFATS Act of 2014 codified the CFATS program into the Homeland Security Act of 2002.

CISA collects the core regulatory data necessary to implement CFATS through the Chemical Security Assessment Tool (CSAT) covered under this collection. For more information about CFATS and CSAT, please visit [www.dhs.gov/chemicalsecurity](http://www.dhs.gov/chemicalsecurity). This information collection (OMB Control No. 1670–0007) will expire on July 31, 2023.<sup>5</sup>

#### Public Participation

OMB is particularly interested in comments that:

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

*Title of Collection:* Chemical Security Assessment Tool.

*OMB Control Number:* 1670–0007.

*Instrument:* Top-Screen.

*Frequency:* “On occasion” and “Other”.

*Affected Public:* Business or other for-profit.

*Number of Respondents:* 3,817 respondents (estimate).

*Estimated Time per Respondent:* 2.04 hours.

*Total Annual Burden Hours:* 7,785 hours.

*Total Annual Burden Cost:* \$703,829.

*Total Annual Burden Cost (capital/startup):* \$0.

*Total Recordkeeping Burden:* \$0.

*Instrument:* Security Vulnerability Assessment and Alternative Security Program submitted in lieu of a Security Vulnerability Assessment.

*Frequency:* “On occasion” and “Other”.

*Affected Public:* Business or other for-profit.

See 6 U.S.C. 621 *et seq.*, as amended by Public Law 116–135, Sec. 16007 (2020).

<sup>5</sup> The currently approved version of this information collection (OMB Control No. 1670–0007) can be viewed at [https://www.reginfo.gov/public/do/PRAViewICR?ref\\_nbr=201905-1670-001](https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201905-1670-001).

*Number of Respondents:* 2,328 respondents (estimate).

*Estimated Time per Respondent:* 1.4136 hours.

*Total Annual Burden Hours:* 3,291 hours.

*Total Annual Burden Cost:* \$297,530.

*Total Annual Burden Cost (capital/startup):* \$0.

*Total Recordkeeping Burden:* \$0.

*Instrument:* Site Security Plan and Alternative Security Program submitted in lieu of a Site Security Plan.

*Frequency:* “On occasion” and “Other”.

*Affected Public:* Business or other for-profit.

*Number of Respondents:* 2,328 (estimate).

*Estimated Time per Respondent:* 7.845 hours.

*Total Annual Burden Hours:* 18,262 hours.

*Total Annual Burden Cost:*

\$1,651,158.

*Total Annual Burden Cost (capital/startup):* \$0.

*Total Recordkeeping Burden:* \$556,040.

*Instrument:* CFATS Help Desk.

*Frequency:* “On occasion” and “Other”.

*Affected Public:* Business or other for-profit.

*Number of Respondents:* 12,000 respondents (estimate).

*Estimated Time per Respondent:* 0.1167 hours.

*Total Annual Burden Hours:* 1,400 hours.

*Total Annual Burden Cost:* \$126,580.

*Total Annual Burden Cost (capital/startup):* \$0.

*Total Recordkeeping Burden:* \$0.

*Instrument:* User Registration.

*Frequency:* “On occasion” and “Other”.

*Affected Public:* Business or other for-profit.

*Number of Respondents:* 1,000 respondents (estimate).

*Estimated Time per Respondent:* 2.5 hours.

*Total Annual Burden Hours:* 2,500 hours.

*Total Annual Burden Cost:* \$226,035.

*Total Annual Burden Cost (capital/startup):* \$0.

*Total Recordkeeping Burden:* \$0.

*Instrument:* Identification of Facilities and Assets at Risk.

*Frequency:* “On occasion” and “Other”.

*Affected Public:* Business or other for-profit.

*Number of Respondents:* 2,252 respondents (estimate).

*Estimated Time per Respondent:* 0.17 hours.

Total Annual Burden Hours: 375 hours.  
 Total Annual Burden Cost: \$33,931.  
 Total Annual Burden Cost (capital/startup): \$0.  
 Total Recordkeeping Burden: \$0.

**Robert Costello,**

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

[FR Doc. 2023-08341 Filed 4-19-23; 8:45 am]

BILLING CODE 9110-9P-P

**DEPARTMENT OF HOMELAND SECURITY**

**Transportation Security Administration**

[Docket No. TSA-2011-0008]

**Request for Applicants for Appointment to the Aviation Security Advisory Committee**

**AGENCY:** Transportation Security Administration, DHS.

**ACTION:** Committee management; request for applicants.

**SUMMARY:** The Transportation Security Administration (TSA) is requesting applications from individuals who are interested in being appointed to serve on the Aviation Security Advisory Committee (ASAC). All applicants must represent one of the constituencies specified below in order to be eligible for appointment. ASAC's mission is to provide advice and recommendations to the TSA Administrator on improving aviation security matters, including developing, refining, and implementing policies, programs, rulemaking, and security directives pertaining to aviation security, while adhering to sensitive security guidelines.

**DATES:** Applications for membership must be submitted to TSA using one of the methods in the **ADDRESSES** section below on or before May 11, 2023.

**ADDRESSES:** Applications must be submitted by one of the following means:

- *Email:* ASAC@tsa.dhs.gov.
- *Mail:* Tamika McCree Elhilali, ASAC Designated Federal Officer, Transportation Security Administration (TSA-28), 6595 Springfield Center Drive, Springfield, VA 20598-6028.

See **SUPPLEMENTARY INFORMATION** for application requirements.

**FOR FURTHER INFORMATION CONTACT:** Tamika McCree Elhilali, ASAC Designated Federal Officer, Transportation Security Administration (TSA-28), 6595 Springfield Center Drive, Springfield, VA 20598-6028, ASAC@tsa.dhs.gov, 202-595-4802.

**SUPPLEMENTARY INFORMATION:** The ASAC is an advisory committee established pursuant to 49 U.S.C. 44946. The committee is composed of individual members representing key constituencies affected by aviation security requirements. As required by statute, the ASAC is composed of individuals representing not more than 34 member organizations.

TSA is seeking applications for the membership categories scheduled to expire in May 2023, which are marked with an asterisk in this section below. Individuals are appointed by the TSA Administrator to represent 19 key constituencies affected by aviation security requirements, as defined at 49 U.S.C. 44946(c)(1)(C). Consistent with applicable law, TSA is committed to pursuing opportunities to appoint a committee that reflects the diversity of the United States. The following list provides the 19 key constituencies and identifies with an asterisk (\*) the constituencies for whom the current representative's term is expiring:

1. Air carriers.
2. All-cargo air transportation.\*
3. Labor organizations representing air carrier employees (3 vacancies).\*
4. Aircraft manufacturers.\*
5. Airport operators.\*
6. General aviation.\*
7. Travel industry.\*
8. Victims of terrorist acts against aviation.
9. Law enforcement and security experts.
10. Indirect air carriers.\*
11. Aviation security technology industry (including screening technology and biometrics).
12. Airport-based businesses.\*
13. Passenger advocacy groups.
14. Airport authorities and businesses that conduct security operations at airports.\*
15. Labor organizations representing transportation security officers.\*
16. Airport construction and maintenance contractors.\*
17. Labor organizations representing employees of airport construction and maintenance contractors.
18. Privacy organizations.
19. Aeronautical repair stations.

Unless otherwise noted, the ASAC does not have a specific number of members allocated to any membership category and the number of members in a category may change to fit the needs of the Committee, but each organization shall be represented by one individual. Members will serve as representatives and speak on behalf of their respective constituency group, and will not be appointed as Special Government Employees as defined in 18 U.S.C.

202(a). Membership on ASAC is personal to the appointee and a member may not send an alternate to a Committee meeting. Pursuant to 49 U.S.C. 44946(c)(3), members shall not receive pay, allowances, or benefits from the Government by reason of their service on ASAC.

**Committee Meetings**

The ASAC typically convenes four times per year. Additional meetings may be held with the approval of the Designated Federal Official. While at least one meeting per year is open to the public, due to the sensitive nature of the material discussed, the other meetings are typically closed to the public. In addition, members are expected to participate on ASAC subcommittees that typically meet more frequently to deliberate and discuss specific aviation matters.

**Committee Membership**

Committee members are appointed by and serve at the pleasure of the TSA Administrator for a 2-year term or until a successor is appointed. Members who are currently serving on the Committee are eligible to reapply for membership. A new application is required.

**Committee Membership Vetting**

All applicants that are presented for appointment to ASAC must successfully complete a Security Threat Assessment (STA) by TSA, as access to sensitive security information will be necessary. U.S. citizens and those meeting residency requirements will be vetted using TSA's Universal Enrollment Services (UES), which includes the collection of biographic and biometric information to allow TSA to perform the STA in regards to criminal history, intelligence, and citizenship. Selected applicants will be offered a no-cost authorization code to complete the three-step UES process; which includes online pre-enrollment, coordinating a visit to an enrollment center, and the in-person visit to the enrollment center.

Non-U.S. applicants presented for appointment to ASAC, will be required to complete additional vetting. This vetting will include the completion and submission of TSA Form 2816B form, and must be submitted at least 30 days prior to visiting TSA spaces.

**Application for Advisory Committee Appointment**

TSA is seeking applications for the membership categories scheduled to expire in May 2023, which are marked with an asterisk in the **SUPPLEMENTARY INFORMATION** section above. Any person wishing to be considered for