SAP Policy may be found in OMB Memorandum 23–04.

- *The SAP Portal:* The SAP Portal is an application interface connecting applicants seeking data with a catalog of metadata for data assets owned by the federal statistical agencies and units. The SAP Portal is not a new data repository or warehouse; confidential data assets will continue to be stored in secure data access facilities owned and hosted by the federal statistical agencies and units. The Portal provides a streamlined application process across agencies, reducing redundancies in the application process.
- *Data Discovery:* Individuals begin the process of accessing restricted use data by discovering confidential data assets through the SAP metadata catalog, maintained by federal statistical agencies at *www.researchdatagov.org.*
- *SAP Portal Application Process:* Individuals who have identified and wish to access confidential data assets apply through the SAP Portal. Applicants must create an account and follow all steps to complete the application. Applicants enter personal, contact, and institutional information for the research team and provide summary information about their proposed project.
- *Submission for Review:* Agencies approve or reject an application within a prompt timeframe. Agencies may also request applicants to revise and resubmit their application.
- *Access to Confidential Data:* Approved applicants are notified through the SAP Portal that their proposal has been accepted. This concludes the SAP Portal process. Agencies will contact approved applicants to initiate completion of their security documents. The completion and submission of the agency's security requirements will take place outside of the SAP Portal.
- *Collection of Information for Data Security Requirements:* In the instance of a positive determination for an application requesting access to an SAMHSA-owned confidential data asset, SAMHSA will contact the applicant(s) to initiate the process of collecting information to fulfill its data security requirements. This process allows SAMHSA to place the applicant(s) in a trusted access category.

Estimate of Burden: The amount of time to complete the agreements and other paperwork that comprise SAMHSA's security requirements will vary based on the confidential data assets requested. To obtain access to SAMHSA confidential data assets, it is estimated that the average time to complete and submit SAMHSA's data security agreements and other paperwork is 40 minutes. This estimate does not include the time needed to complete and submit an application within the SAP Portal. All efforts related to SAP Portal applications occur prior to and separate from SAMHSA's effort to collect information related to data security requirements.

The expected number of applications in the SAP Portal that receive a positive determination from SAMHSA in a given year may vary. Overall, per year, SAMHSA estimates it will collect data security information for 15 application submissions that received a positive determination within the SAP Portal. SAMHSA estimates that the total burden for the collection of information for data security requirements over the course of the three-year OMB clearance will be about 30 hours and, as a result, an average annual burden of 10 hours.

Comments: As required by 5 CFR 1320.8(d), comments on the information collection activities as part of this study were solicited through the publication of a 60-Day Notice in the **Federal Register** at [insert FR citation]. SAMHSA received [number] comments, to which we here respond.

Updates: This section is needed if there have been any major changes since the first FRN was published, for example, if estimates of burden (in terms of hours or respondents), scope, sampling, etc. were changed. Outline what the initial FRN specified, the new information, and the reason(s) why it changed.

Carlos Graham,

Reports Clearance Officer.

[FR Doc. 2023–17176 Filed 8–9–23; 8:45 am]

BILLING CODE 4162–20–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2023–0019]

Agency Information Collection Activities: ReadySetCyber Initiative Questionnaire

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

ACTION: 60-Day notice and request for comments on a new collection.

SUMMARY: CISA will submit 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 October 10, 2023.

ADDRESSES: You may submit comments, identified by docket number Docket # CISA–2023–0019, 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 # CISA–2023–0019. 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://www.regulations.gov.*

SUPPLEMENTARY INFORMATION: Consistent with CISA's authorities to ''carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States'' at 6 U.S.C. 652(e)(1)(B) and provide federal and non-federal entities with ''operational and timely technical assistance'' at 6 U.S.C. 659(c)(6) and ''recommendation on security and resilience measures'' at 6 U.S.C. 659(c)(7), CISA's ReadySetCyber Initiative will collect information in order to provide tailored technical assistance, services and resources to critical infrastructure (CI) organizations and state, local, tribal, and territorial (SLTT) governments based on the characteristics of their respective cybersecurity programs. CISA seeks to collect this information from US CI and SLTT organizations on a voluntary and fully electronic basis so that each organization can be best supported in receiving tailored cybersecurity recommendations and services.

The overarching goal of CISA's ReadySetCyber Initiative is to help CI and SLTT organizations access information and services that are tailored to their specific cybersecurity needs. In addition, CISA expects this initiative to yield several additional benefits, including:

- Further adoption of CISA's Cybersecurity Performance Goals (CPGs) as the default approach for assessing Organizational progress and identify prioritized cybersecurity gaps;
- Collection of information about organizations' cybersecurity posture and progress, enabling more targeted engagement with sectors, regions, and individual organizations;
- More effective allocation of capacity-constrained services to specific stakeholders;
- Provision of a simplified approach to the guiding stakeholders into enrollment for, scalable services and rapidly expand uptake thereof; and

- Furthering the development of relationships between CI and SLTT organizations and CISA's regional cybersecurity personnel.

CISA's CPGs are a set of voluntary cybersecurity practices which aim to reduce the risk of cybersecurity threats to U.S. CI and SLTT organizations. CISA offers services and resources to aid CI and SLTT organizations in adopting the CPGs and seeks to make accessing appropriate services and resources as efficient as possible, especially for organizations whose cybersecurity programs operate at low levels of capability.

For example, an organization that is unsure of its ability to enumerate all of its internet-facing sites and services could leverage CISA's highly scalable automated testing services to scan its entire network range. Organizations with cybersecurity programs with more advanced characteristics who wish to evaluate their network segmentation controls are better positioned to take advantage of CISA's more resource-intensive architecture assessments. All organizations completing the questionnaire will also be connected with a CISA cybersecurity representative in their jurisdiction to provide direct support and engagement.

To measure adoption of the CPGs and assist CI and SLTT organizations in finding the most impactful services and resources for their cybersecurity programs, CISA is seeking to establish a voluntary information collection that uses respondents' answers to tailor a recommended package of services and resources most applicable to their evaluated level of program capability. Without collecting this information, CISA would be unable to tailor an appropriate suite of services, recommendations, and resources to assist the organization in protecting itself against cybersecurity threats, thereby creating burdens of inefficiency for service requesters and CISA alike.

In addition, receipt of this information is critical to CISA's ability to measure the adoption of CISA's CPGs by CI and SLTT organizations. The information to be collected will address various inquiries, such as: whether an organization keeps a regularly updated inventory of all assets with an internet Protocol address; the types of incident reporting and vulnerability disclosures required by an organizations' contracts with its vendors and suppliers; and whether the entity requires a minimum password strength required for all password-protected assets.

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 via 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: ReadySetCyber.

OMB Number:

Frequency: Upon each voluntary request for technical assistance, which CISA expects to occur on an annual basis.

Affected Public: Critical Infrastructure Owners & Operators seeking CISA services.

Number of Respondents: Approximately 2,000 per year.

Estimated Time per Respondent: 20 Minutes.

Total Burden Hours: 666.7 Hours.

Robert J. Costello,

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

[FR Doc. 2023–17183 Filed 8–9–23; 8:45 am]

BILLING CODE 9110–09–P

DEPARTMENT OF THE INTERIOR

National Park Service

[NPS–WASO–NAGPRA–NPS0036326; PPWOCRADN0–PCU00RP14.R50000]

Notice of Inventory Completion: Oberlin College, Oberlin, OH

AGENCY: National Park Service, Interior.

ACTION: Notice.

SUMMARY: In accordance with the Native American Graves Protection and Repatriation Act (NAGPRA), Oberlin College has completed an inventory of human remains and has determined that there is a cultural affiliation between the human remains and Indian Tribes or Native Hawaiian organizations in this notice. The human remains were removed from the Hawaiian Islands, HI.

DATES: Repatriation of the human remains in this notice may occur on or after September 11, 2023.

ADDRESSES: Dr. Amy V. Margaris, Oberlin College, King Building, 10 N. Professor Street, Oberlin, OH 44074, telephone (440) 775–5173, email *amy.margaris@oberlin.edu.*

SUPPLEMENTARY INFORMATION: This notice is published as part of the National Park Service's administrative responsibilities under NAGPRA. The determinations in this notice are the sole responsibility of Oberlin College. The National Park Service is not responsible for the determinations in this notice. Additional information on the determinations in this notice, including the results of consultation, can be found in the inventory or related records held by Oberlin College.

Description

Human remains representing, at minimum, one individual were removed from the Hawaiian Islands, HI. Accession #65 in the accession book of the former Oberlin College Museum records that in August of 1875, Mr. E. P. Church of Greenville, Michigan donated to the Museum one ''Skull of Hawaiian, Cave Burial Place, Hawaiian Islands.'' According to records of the Oberlin College Archives, E. P. Church was an 1863 graduate of Oberlin College who lived on O'ahu from 1865–1875. He served as Professor of Mathematics at Oahu College (now Punahou School) in Honolulu, Hawaii (1865–1871) and as President of Oahu College (1871–1875). The human remains were retained by Oberlin College after the Museum's closure in the 1950s, and they are now in the care of the Oberlin College Department of Anthropology. The human remains consist of a skull belonging to an adult of indeterminate age and sex. No associated funerary remains are present.

Cultural Affiliation

The human remains in this notice are connected to one or more identifiable earlier groups, tribes, peoples, or cultures. There is a relationship of shared group identity between the identifiable earlier groups, tribes, peoples, or cultures and one or more Indian Tribes or Native Hawaiian organizations. The following types of information were used to reasonably trace the relationship: archeological, biological, cultural, geographical, and historical.