U.S. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY	**Cybersecurity and Infrastructure Security Agency Vulnerability Assessments**	OMB Control Number: 1670-0035 OMB Expiration Date: 01/31/2020

Who must comply?	The information collected in the Cybersecurity and Infrastructure Security Agency (CISA) Vulnerability Assessments is voluntarily, but full completion of the assessment data is required for an organization to receive a complete evaluation of their security posture. The information is collected by Protective Security Advisors (PSA), Cyber Security Advisors (CSA), or by the organization itself.
What is this collection about?	Protective Security Advisors (PSAs) and Cyber Security Advisors (CSAs) conduct voluntary assessments on CI facilities. These assessments are web-based and are used to collect an organization's basic, high-level information, and its dependencies.
Where do I find the requirements for this information?	The Presidential Policy Directive-21 (PPD-21) (2013) and the National Infrastructure Protection Plan (NIPP) (2013) 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 a data collection system that contains several capabilities which support the homeland security mission in the area of critical infrastructure (CI) protection.
How is the information submitted?	The collection of information uses automated electronic vulnerability assessments and questionnaires. The vulnerability assessments and questionnaires are electronic in nature and include questions that measure the security, resiliency and dependencies of an organization. The vulnerability assessments are arranged at the request of an organization and are then scheduled and performed by a PSA or CSA.
What happens when complete information is received?	This data is used to determine a Protective Measures Index (PMI) and a Resilience Measures Index (RMI) for the assessed organization. This information allows an organization to see how it compares to other organizations within the same sector as well as allows them to see how adjusting certain aspects would change their score. This allows the organization to then determine where best to allocate funding and perform other high-level decision-making processes pertaining to the security and resiliency of the organization.
For additional information, contact--	For specific questions related to collection activities, please contact IPGatewayHelpDesk@hq.dhs.gov

Paperwork Burden Disclosure Notice:

Public reporting burden for this data collection is estimated to take 7.5 hours per response for assessments and 10 minutes per response for post-assessment questionnaires. The burden estimate includes the time reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and submitting this form. This collection of information is required to obtain or retain benefits. You are not required to respond to this collection of information unless a valid OMB control number is displayed on this form. Send comments regarding the accuracy of the burden estimate and any suggestion for reducing the burden to: Information Collections Management, DHS/CISA, IPGatewayHelpDesk@hq.dhs.gov, ATTN: PRA 1670-0035. NOTE: DO NOT send your completed form to this address.

Privacy Notice:
Authority: 44 U.S.C. 3101 and 44 U.S.C. 3534 authorize the collection of information.
Purpose: DHS will use this information to create and manage your user account and grant access to the Infrastructure Protection (IP) Gateway.
Routine Uses: This information may be disclosed as generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974. This inclufes using the information, as necessary and authorized by the routine uses published in DHS/ALL-004 – General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 Fed. Reg. 70,792.
Disclosure: Furnishing this information is voluntary; however, failure to provide the information requested may delay or prevent DHS from processing your access request.

An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number.
The Coast Guard estimates that the average burden per response for this report varies per information collection—about 1.5 hours for a new tank vessel VCS submission; and 2 hours for a certifying entity submission; and up to 7 hours for a VCS facility response. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: Commandant (CG-ENG), U.S. Coast Guard Stop 7509, 2703 Martin Luther King Jr Ave SE, Washington, DC 20593-7509 or Office of Management and Budget, Paperwork Reduction Project (1625-0060), Washington, DC 20503.