CISA | Assessments Service Request Form

OMB #1670-XXXX exp.

Organization Name

Organization Customer Segment

-

Organization Headquarters Address

Organization Assessment Point of Contact Name

State

Organization Assessment Point of Contact Email

United States of America

Does this request include Election Infrastructure Systems? ◯ Yes ◉ No

Which Critical Infrastructure Sector(s) does your organization most closely align with?

-

-

-

The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy (How do I find my NAICS code?)

Please provide your organization's primary NAICS code (Optional):

Please provide any additional NAICS codes associated with your organization (Optional):

Category of Assets/Networks to be assessed (select all the apply):

- ☐ Informational Technology (IT)
- ☐ Operational Technology (OT-- ICS and SCADA)
- ☐ Cloud Infrastructure (CI)
- ☐ Virtual Environment (VE)

Would your organization like to enroll in Cyber Hygiene Vulnerability Scanning?

Note: All services are available at no cost to federal agencies, state, local, tribal and territorial governments, critical infrastructure, and private organizations. Additional information can be found on the Cyber Resources Hub at cisa.gov/cyber-hygiene-services.

☐ Yes, we would like to enroll in Vulnerability Scanning

PRA Burden Statement: The public reporting burden to complete this information collection is estimated at 6.6 minutes per response, including the time completing and reviewing the collected information. The collection of this information is voluntary. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/CISA. Mail Stop 0608, 245 Murray Lane SW, Arlington, VA 20598. ATTN: PRA [1670-00XX].

Privacy Act Statement: Authority: 6 U.S.C. § 659(c)(6) authorize the collection of this information.

Purpose: The primary purpose for the collection of this information is to allow the Department of Homeland Security Cybersecurity and Infrastructure Security Agency to contact you about your request.

Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System November 25, 2008, 73 FR 71659.

Disclosure: Providing this information is voluntary. However, failure to provide this information will prevent CISA from contacting you in the event there are questions about your request.

CISA | Assessments Service Request Form

Organization Questions

The below questions are not required to receive Cyber Hygiene Vulnerability Scanning. CISA is collecting this information in order to tailor further service offerings to your organization and gain a better understanding of CISA's critical infrastructure partners.

How many employees are in your organization?

How many IT/ICS management and staff members are dedicated to your organization?

Does your organization have a dedicated Security Operations Center?

Does your organization have the internal capability to respond to incidents? Yes ☐ No ☐

How does your organization allocate resources to cybersecurity? Yes ☐ No ☐

How many users in your organization utilize the networks you are hoping for CISA to assess?

How many customers does your organization serve?

Is your organization seeking assessments in any of the below security areas?

- ☐ External and perimeter network configurations
- ☐ Security architecture
- ☐ Web application security
- ☐ Internal network configurations
- ☐ Blue team and SOC capabilities
- ☐ Phishing prevention

If you selected OT (ICS/SCADA) on page 1, please answer the questions below: N/A ☐

Does your organization have current logical network diagrams? Yes ◯ No ◯

Does your organization have managed network infrastructure devices (switch, router, firewall) at the IT/OT system demarcation points to facilitate header-only packet capture? Yes ◯ No ◯

Does your organization have network admin staff that can use products such as Wireshark or T-shark to perform packet captures? Yes ◯ No ◯

What are the predominant OT protocols (i.e. Modbus, DNP3, PROFIBUS and PROFINET, BACnet, etc.) in use?

Would you like to discuss the possibility of CISA working with your staff to facilitate network packet captures? Yes ◯ No ◯