PRA Practice

OMB Control Number: 1670-0027
OMB Expiration Date: 5/31/2024

PRA Burden Statement: The public reporting burden to complete this information collection is estimated at 16 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 [1670-0027].

Start of Block: Demographic & Geographic Questions

OMB Number: 1670-0027

Critical Infrastructure Commercial Shared Services Survey

Critical Infrastructure Commercial Shared Services Survey
Privacy Act Statement

Authority: 6 U.S.C. § 652(c) (2), (5) and (11) and E.O. 14058 of December 13, 2021 authorize the collection of this information.

Purpose: The primary purpose for the collection of information is to solicit feedback on the cybersecurity maturity of Critical Infrastructure entities that partner with the Cybersecurity and Infrastructure Security Agency (CISA) or have an interest in partnering with CISA.

Routine Uses: The information collected may be disclosed externally as a “routine use” pursuant to, 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 may prevent CISA from contacting you regarding your submission.

Q1 Enter your organization's formal name (no acronyms)

_____

Q2 List your organization's headquarters location information:

- O State / Territory / Tribe _____

Q3 Estimate the number of personnel in your organization:

- O 0-10
- O 11-25
- O 26-50
- O 51-100
- O 101-200
- O 201-400
- O 401-1000
- O 1001+

Q4 How many people does your organization serve / support?

- O Fewer than 2,500
- O 2,501 - 4,999
- O 5,000 - 9,999
- O 10,000 - 24,999
- O 25,000 - 249,999
- O 250,000 - 1 million
- O More than 1 million

Q5 What sector best describes your organization?

- ☐ Chemical
- ☐ Commercial Facilities
- ☐ Communications
- ☐ Critical Manufacturing
- ☐ Dams
- ☐ Defense Industrial Base
- ☐ Emergency Services
- ☐ Energy

- [ ] Financial Services
- [ ] Food and Agriculture
- [ ] Government Facilities
- [ ] Healthcare and Public Health
- [ ] Information Technology
- [ ] Nuclear Reactors, Materials, and Waste
- [ ] Transportation
- [ ] Waste and Wastewater Systems

Q6 How does your organization currently engage with CISA?

- [ ] Uses CISA services (please specify)

_____

- [ ] Reports incidents to CISA
- [ ] Receives 1:1 technical support
- [ ] Reviews and follows CISA guidance
- [ ] My organization does not currently have a relationship/engage with CISA
- [ ] Other _____

Q7 To help inform CISA's future service offerings, would you use any of these services if CISA offered them?

- [ ] Security Operations/SOC optimization and maturity
- [ ] Modernization (i.e., migration of legacy applications to the cloud / zero trust)
- [ ] Identity and Access Capabilities
- [ ] Governance, Risk, and Compliance Capabilities
- [ ] Dedicated Technical/cyber training and Skilling
- [ ] Incident Response and Threat intelligence capabilities
- [ ] Data accuracy, quality, and/or automated reporting
- [ ] Offensive Security/Red Team (penetration testing, tabletop simulations, etc.)
- [ ] Vulnerability Management

- [ ] Data Backup & Asset Recovery
- [ ] Other: Please explain

Page Break

End of Block: Demographic & Geographic Questions

Start of Block: Sector Specific Questions

Q8 To inform the development of future CISA products and services what are still the greatest challenges you face to fulfilling cybersecurity goals?

- ☐ Immature cyber culture and organizational governance
- ☐ Lack of Technical Capabilities
- ☐ Threat of Large Advanced Persistent Threats (APTs)
- ☐ Insufficient Staffing / Coverage
- ☐ Other _____

Q9 What training or guidance product can the Cybersecurity Infrastructure Security Agency (CISA) provide to best support your organization?

- ☐ Policy _____
- ☐ Universal Standards
- ☐ Voluntary cost-free Managed services
- ☐ Convening similar partners to discuss challenges/best practices
- ☐ Other _____

- ○ No we do not

Q10 To help shape CISA's service offerings, would your organization benefit from guidance about creating a Vulnerability Disclosure Policy?

- O Yes
- O No

Q11 After receiving services from CISA, does your organization understand the importance of keeping user and administrator, or super-user accounts separate?

- O Yes, absolutely
- O Yes, mostly
- O No we do not
- O Other _____

Q12 After receiving services from CISA, does your organization understand the importance of re-evaluating all user and administrator, or super-user account privileges on a recurring basis?

- O Yes, absolutely
- O Yes, mostly
- O No we do not
- O Other _____

Q13 After receiving services from CISA, does your organization understand the importance of isolating Operational Technology (OT) assets from the public Internet, except where explicitly required for operation and protected by appropriate compensating controls?

O Yes, absolutely

O Yes, mostly

O No we do not

O Other _____

Q14 To help CISA scope future service offerings, would your organization benefit from guidance or instruction about implementing an enforced offboarding process to help ensure all departing employees lose network accesses on the day of their departure?

O Yes, absolutely

O Yes, mostly

O No we do not

O Other _____

Q15 Would your organization find it helpful if CISA were to offer policies and procedure templates to assist in prohibiting the connection of unauthorized devices and media to Information Technology systems?
Yes
No
Unsure

_____

_____

Q16 What new or improved capability provided by CISA would help your organization the most improve its cybersecurity posture?

- O Vulnerability Disclosure Platform
- O Protective Domain Name System Resolver (DNS)
- O Operational/Threat Information Sharing
- O Assessment Services
- O Community Information Sharing and Exchange
- O Guidance
- O Incident Response Support
- O Security Operations Center (SOC) Support
- O Other _____

Q17 Did your organization experience any challenges sharing the necessary data with CISA for proper operation of [insert CISA service or program name]?

O Yes

O No

Q18) If yes, explain: _____

End of Block: Sector Specific Questions