CYBER SECURITY ADVISORS (CSA)

CYBER INFRASTRUCTURE SURVEY (CIS) POST-ASSESSMENT QUESTIONNAIRE

Thank you for completing the Cyber Infrastructure Survey post-assessment questionnaire. For more information about this questionnaire or about the Cybersecurity Advisors Program, please contact Tara Brewer at cyberadvisor@hq.dhs.gov

Cybersecurity Motivation

What was your organization's motivation to participate in the CIS? (select all that apply)

- ☐ Validate a Finding
- ☐ Review Compliance
- ☐ Response to Incident within Organization
- ☐ Reinforce Standards
- ☐ Proactive Cybersecurity Assessment/Start of Improvement Effort
- ☐ Obtain Professional Third-Party Opinion of Cyber Defenses
- ☐ Response to Incident within Industry
- ☐ Other:

Survey Impact

In which of the following CIS domains has your organization planned, scheduled, or implemented at least one improvement?

	N/A	Planned	Scheduled	Implemented
Cybersecurity Management Leadership roles and responsibilities, documentation, lifecycle tracking, information sharing, accreditation, assessment, and audits	○	○	○	○
Cybersecurity Forces Personnel assigned to maintain and operate critical services	○	○	○	○
Cybersecurity Controls An effective baseline of security controls governing the critical service	○	○	○	○
Incident Response Preparation for an incident that affects the critical service	○	○	○	○
Dependencies Critical service's dependence on data generated or stored by a system and the organization's mitigating controls and procedures	○	○	○	○

As a result of the CIS, has your organization...

Improved its allocation of its overall IT and/or cybersecurity budget?
○ Yes | ○ No

Established or changed your targeted cybersecurity posture?
○ Yes | ○ No

Shared cybersecurity information with external parties?
○ Yes | ○ No

If Yes, what information is shared:
- ☐ Lessons Learned ☐ Best Practices ☐ Training Tips
- ☐ Other:

Leveraged the NIST Cybersecurity Framework?
○ Yes | ○ No

Please provide a brief explanation for any improvements or changes listed above:

[redacted]

Quality of Survey & Dashboard

Did DHS establish expectations through CIS preparations? ○ Yes | ○ No

	Strongly Agree		Neither Agree nor Disagree		Strongly Disagree	Explanation:
The dashboard was comprehensible, readable, and usable.	○	○	○	○	○	
The dashboard was valuable.	○	○	○	○	○	
The survey met my organization's expectations.	○	○	○	○	○	

How could the CIS be improved?

How could the CIS *dashboard* be improved?

Next Steps

Is your organization interested in participating in additional DHS cyber assessments or other services? (select all that apply)

A Re-Assessment of the Same Critical Service:
- ☐ Cyber Resilience Review (CRR)
- ☐ External Dependencies Management (EDM)
- ☐ Cyber Infrastructure Survey (CIS)

A New Assessment of a Different Critical Service:
- ☐ Cyber Resilience Review (CRR)
- ☐ External Dependencies Management (EDM)
- ☐ Cyber Infrastructure Survey (CIS)

Another DHS Service:
- ☐ Phishing Campaign Assessment
- ☐ Network Risk and Vulnerability Assessment
- ☐ Cybersecurity Evaluation Tool
- ☐ Industrial Control Systems Evaluation
- ☐ Cyber Hygiene Scanning