Homeland Security

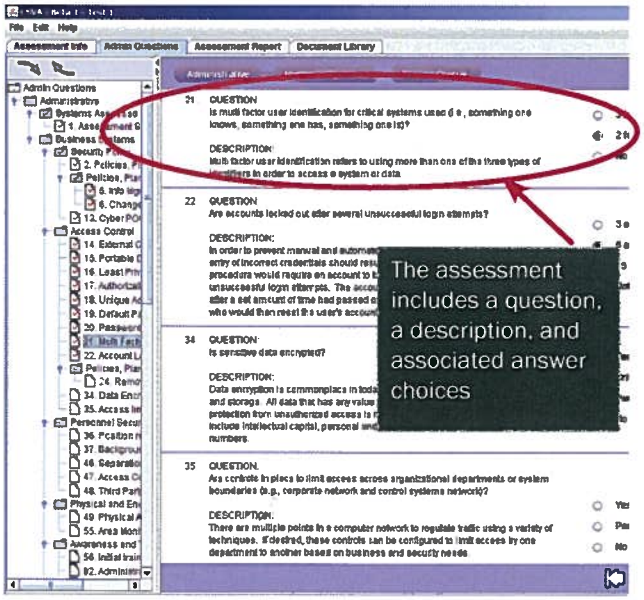
Cyber Security Vulnerability Assessment

The Department of Homeland Security (DHS) is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. The National Cyber Security Division (NCSD) is the Department's lead agency for securing cyberspace and our Nation's cyber assets and networks.

Cyber Security Vulnerability Assessment Supports Sectors' Critical Infrastructure Protection Efforts

Critical infrastructures are dependent on information technology systems and computer networks for essential operations. Particular emphasis should be placed on the reliability and resiliency of the systems that comprise and interconnect these infrastructures. NCSD collaborates with partners from across public, private, and international communities to advance this goal by developing and implementing coordinated security measures to protect against physical and cyber threats.

NCSD develops guidance and tools to assist critical infrastructure owners and operators in assessing and managing their cyber risks. One of these tools, the Cyber Security Vulnerability Assessment (CSVA), enables organizations and facilities to self-assess their overall cyber security posture.



21 QUESTION
Is multi factor user identification for critical systems used (i.e., something one knows, something one has, something one is)?

DESCRIPTION:
Multi factor user identification refers to using more than one of the three types of identifiers in order to access a system or data

22 QUESTION
Are accounts locked out after several unsuccessful login attempts?

DESCRIPTION:
In order to prevent manual and automa… entry of incorrect credentials should resu… procedure would require an account to b… unsuccessful login attempts. The accou… after a set amount of time had passed o… who would then reset the user's accoun…

34 QUESTION
Is sensitive data encrypted?

DESCRIPTION:
Data encryption is commonplace in toda… and storage. All data that has any value… protection from unauthorized access is n… include intellectual capital, personal and… numbers.

35 QUESTION
Are controls in place to limit access across organizational departments or system boundaries (e.g., corporate network and control systems network)?

DESCRIPTION:
There are multiple points in a computer network to regulate traffic using a variety of techniques. If desired, these controls can be configured to limit access by one department to another based on business and security needs

○ Yes
○ Par
○ No

The assessment includes a question, a description, and associated answer choices

The CSVA evaluates the policies, plans, and procedures in place to reduce cyber vulnerabilities for business and control systems. It consists of approximately 100 multiple choice questions across ten categories. Based on these responses, the CSVA identifies effective practices and suggests options that an organization or facility can implement to enhance their cyber security. The assessment questions and results are applicable for all critical infrastructure sectors

The CSVA leverages recognized standards, guidance, and methodologies from organizations, such as the International Organization for Standardization, the Information Systems Audit and Control Association, and the National Institute of Standards and Technology. The CSVA's content has been reviewed and refined with security partners with cyber expertise in multiple critical infrastructure sectors, and it continues to be updated and enhanced as security standards and practices evolve.

Key Benefits

- Contributes to organizations' or facilities' risk management and decision-making activities
- No information is shared with DHS or other government entities; results are intended for organizational use only
- Results can be voluntarily shared with NCSD to obtain further insight and expertise
- Uses a repeatable approach to assess an organization's or facility's cyber security posture to enable comparison across different facilities or over several years
- Raises awareness and facilitates discussion on cyber security

If you would like to learn more about the CSVA or obtain a copy, please contact NCSD's Critical Infrastructure Protection Cyber Security Program via e-mail at ncsd_cipcs@hq.dhs.gov.[1]

[1] *The CSVA has been prepared by NCSD for use by government and industry on a voluntary basis and is not subject to copyright (attribution would be appreciated by NCSD). The information in the CSVA should not be taken to contradict standards and guidelines made mandatory and binding by Federal agencies.*