Default Question Block

Your participation is requested in a risk assessment survey on: **Cyber Attacks on Physical Infrastructure.**

DHS is applying Multi-Criteria Decision Analysis (MCDA) to prioritize emerging risks to the Homeland. Your responses will be used to rank 12 emerging risks. This survey is part of a larger effort to assist DHS in evaluating methodologies for characterizing and ranking emerging risks.

This survey is completely voluntary, and you can opt out of the entire survey or portions of it at any time.

This survey is not classified or confidential. Only the MITRE team will have access to individual responses; they will summarize the raw data and provide DHS with only summarized results that are not attributable to any one of the respondents.

The deadline for completion of this survey is **August 28, 2020**.

If you have any questions about this survey, please contact the MITRE Project Leader, Gabriella Nicastro, at gabriella@mitre.org.

Block 1

This is the survey on: Cyber Attacks on Physical Infrastructure

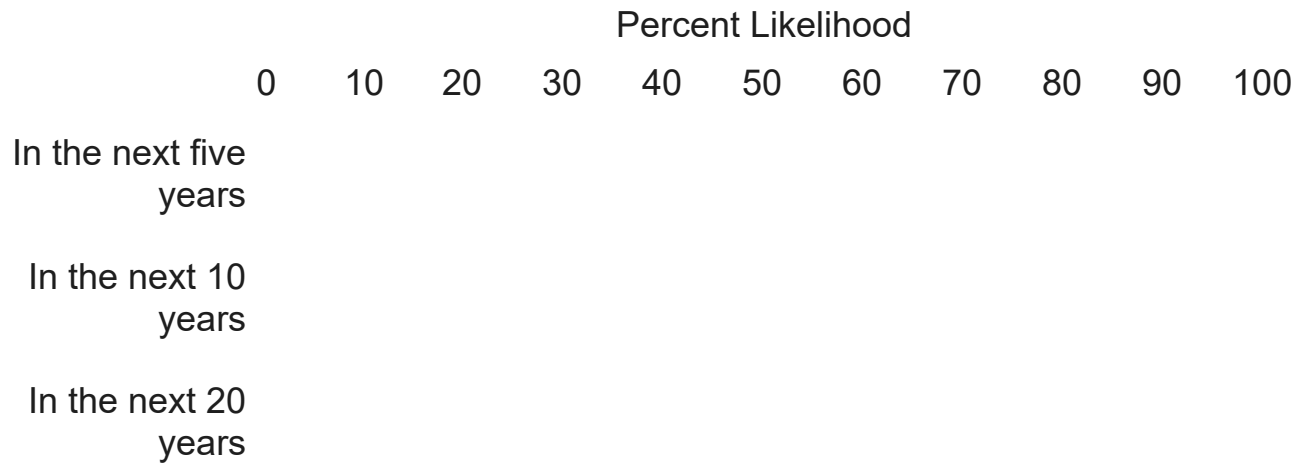
Cyber Attacks on Physical Infrastructure is defined as: An attempt by third parties, possibly adversaries, to damage or destroy a computer network or system, to damage the infrastructure controlled by the system, or gain access to unauthorized information.

THREAT

Likelihood of Occurrence Within Several Possible Timeframes

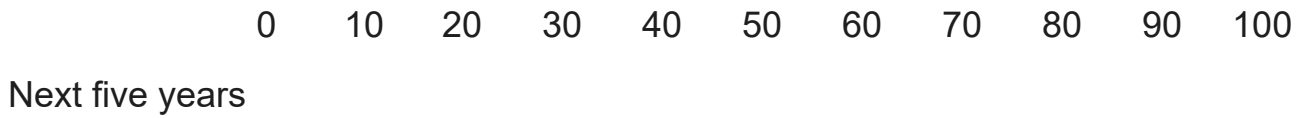
Please rate the likelihood that a threat from Cyber Attacks on Physical Infrastructure will occur within each timeframe below.

	Percent Likelihood										
	0	10	20	30	40	50	60	70	80	90	100
In the next year											



Likelihood of Origination

Rate the likelihood that an adversary would be able to obtain and use Cyber Attacks on Physical Infrastructure to cause harm in the next five years, assuming Cyber Attacks on Physical Infrastructure exists.



Ability to Anticipate

A threat from Cyber Attacks on Physical Infrastructure could be anticipated in a timeframe that would enable effective risk management.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Capacity for Mitigation

Capacity for mitigation is the ability to apply a complete and diverse range of techniques to reduce the adverse effects of, or prevent the occurrence of, a potential threat event. This could include implementing policies, procedures, or preventive actions like education and monitoring.

The US Government has capacity for mitigation of threat from Cyber Attacks on Physical Infrastructure.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

DHS has capacity for mitigation of threat from Cyber Attacks on Physical Infrastructure.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

VULNERABILITY

Vulnerabilities in Information Domain

An information domain vulnerability is a weakness in the information system that creates a threat opportunity. Such vulnerabilities may include those in data security, information use and processing, or internal controls. Information domain vulnerabilities may result in loss of data, altered data, intellectual property theft, or other negative outcomes.

Cyber Attacks on Physical Infrastructure will exploit or create vulnerabilities in the information domain.

- ◯ Strongly disagree
- ◯ Somewhat disagree

- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Vulnerabilities in Physical Domain

A physical domain vulnerability is a weakness in a system's infrastructure that, if disrupted, could result in its destruction or failure.

Cyber Attacks on Physical Infrastructure will exploit vulnerabilities in the physical domain.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Vulnerabilities in Social Domain

A social domain vulnerability is a weakness within the human component of a critical system, that, if exploited, could result in significant damage to the system.

Cyber Attacks on Physical Infrastructure will exploit vulnerabilities in the social domain.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

CONSEQUENCES

Economic Impact

Economic impact includes economic depression, recession, monetary cost to the government, trade disruption, or rise in unemployment.

The economic impact of an occurrence of Cyber Attacks on Physical Infrastructure would be:

- ◯ Not at all severe
- ◯ Slightly severe
- ◯ Somewhat severe
- ◯ Moderately severe
- ◯ Extremely severe

Environmental Impact

Environmental impact is an adverse change to the ecosystem as a direct or indirect result of human actions.

The environmental impact of an occurrence of Cyber Attacks on Physical Infrastructure would be:

- ◯ Not at all severe
- ◯ Slightly severe
- ◯ Somewhat severe
- ◯ Moderately severe
- ◯ Extremely severe

Health Impact and Fatalities

Health impact and fatalities includes human death, injury, or sickness, or stress on medical facilities.

Health impacts and fatalities resulting from an occurrence of Cyber Attacks on Physical Infrastructure would be:

- ◯ Not at all severe
- ◯ Slightly severe
- ◯ Somewhat severe

- ◯ Moderately severe
- ◯ Extremely severe

The number of fatalities resulting from an occurrence of Cyber Attacks on Physical Infrastructure would be:

- ◯ 0-999 individuals
- ◯ 1,000-9,999 individuals
- ◯ 10,000-99,999 individuals
- ◯ 100,000-999,999 individuals
- ◯ More than 1,000,000 individuals

The number of persons injured or made ill by an occurrence of Cyber Attacks on Physical Infrastructure would be:

- ◯ 0-999 individuals
- ◯ 1,000-9,999 individuals
- ◯ 10,000-99,999 individuals
- ◯ 100,000-999,999 individuals
- ◯ More than 1,000,000 individuals

Social Impact

Social impact includes direct effects within the Homeland such as loss of confidence in government, civil unrest, scapegoating, and hunger.

The social impact of a threat event from Cyber Attacks on Physical Infrastructure would be:

- ◯ Not at all severe
- ◯ Slightly severe
- ◯ Somewhat severe
- ◯ Moderately severe
- ◯ Extremely severe

RESILIENCE

Ability to Adapt

Ability to adapt refers to the capability to adjust to new conditions.

Once a threat event from Cyber Attacks on Physical Infrastructure occurs, the United States' ability to adapt would be easy.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree

- ◯ Somewhat agree
- ◯ Strongly agree

Ability to Recover

After the occurrence of a threat event from Cyber Attacks on Physical Infrastructure, what is the time required to return to a normal condition or state?

- ◯ Less than 1 year
- ◯ 1 to 5 years
- ◯ 6 to 10 years
- ◯ 11 to 20 years
- ◯ Over 20 years or never

Please click below to submit and record your responses.

Powered by Qualtrics