The CISA Cybersecurity Strategic Plan FY2024 – 2026 underscores the 'Whole of Nation' mission in cybersecurity. Reflect on the roles and responsibilities of various entities under this approach, from individual citizens to governmental bodies. How can this collective strategy effectively mitigate cyber risks, and where might challenges arise?

Under the CISA Cybersecurity Strategic Plan from 2024 to 2026, various entities bear different roles and responsibilities. The three main goals are to address immediate threats, harden the terrain, and drive security at scale. Of course, accomplishing these goals would require the assistance of both public and private sectors.

There are several ways that this collective strategy can effectively mitigate cyber risks or threats. CISA's approach to cybersecurity is already collaborative. CISA (n.d.) states that they maintain operation partnerships with agencies such as the FBI, NSA, USCYBERCOM, and even the OMB. Within cybersecurity, there is a strategy called "defense-in-depth," where different layers of security protect different systems, because no single layer can defend against every type of threat. To me, CISA's collaborative approach is similar to "defense-in-depth" because several agencies cooperate with each other (and this may even include sharing cyber threat info) to raise national defense and awareness. All the listed agencies could also be valuable targets, so if they were to cooperate with each other, they would strengthen their links together.

Down to the objectives, objective 1.3 exemplifies CISA's approach. The objective invigorates the role of the Computer Emergency Response Team (CERT) to be more responsive, and the Joint Cyber Defense Collaboration serves to ally the government, the private sector, and foreign partners. Additionally, CISA also plans to develop and execute cyber defense plans with these partners. More participants means more security.

Objective 2.1's goal is to "inform, guide, and drive adoption of the most impactful cybersecurity measures by first understanding how attacks occur," and this knowledge will help inform security decisions not only for the government but also for the private sector (CISA, n.d.). Objective 2.2 drives effective cybersecurity measurements, and objective 2.3 is about CISA providing services for organizations in need (e.g., "target rich, resource poor"). Overall, the main intent is national collaboration.

However, there are some challenges that arise and can impact the effectiveness of this strategy. CISA may not be able to assist every "target-rich, resource-poor" organization, as there are hundreds if not thousands of organizations needing cybersecurity services. It is not feasible to help every organization. Additionally, considering objective 2.1's goal of informing security decisions, private sector organizations may not actually learn from CISA informing them, and they fail to effectively apply their security. Moreover, objective 3.1 is about CISA promoting trustworthy technology, or technologies that have been developed with security in mind. Is the private sector willing to set aside profits in exchange for cybersecurity? It would require

monumental effort to influence these companies in changing their focus. Ultimately, many of these challenges boil down to logistics or human issues.

References:

CISA. (n.d.). *FY2024-2026 Cybersecurity Strategic Plan*.

https://www.cisa.gov/sites/default/files/2025-01/FY2024-2026_Cybersecurity_Strategic_Plan508.pdf

CLASSMATE RESPONSE:

Hello, Brandon.

You pretty much summarized the benefits and weaknesses of this “whole of nation” approach. CISA’s Cybersecurity Strategy Plan prioritizes large private companies because of their larger resource pools, but it also targets “target rich, resource poor” organizations to, as you stated, achieve defense-in-depth. Essentially, in this plan, the goal is for everyone, from the macro to the micro level, to be knowledgeable and proactive in cybersecurity. In fact, one of the objectives enforces regulations that will promote security by design. However, there are several potential issues. How willing are organizations to prioritize security over profit, and do they see security as profitable? Are individuals willing to actually learn about basic cybersecurity/security practices? CISA and other government agencies can only do so much. If we had, as a nation, a culture that promotes and is knowledgeable about cybersecurity, ignorance and negligence wouldn’t be so big of a problem.