Establish Regional Cybersecurity Centers of Excellence

Background: While public and private sector awareness of cybersecurity vulnerabilities has increased over the last two decades, the Nation remains increasingly exposed to elevated levels of risk due to cybersecurity gaps and weaknesses. This is true across the 16 sectors of critical infrastructure (e.g., election systems, electrical grids, hospitals, airports, etc.). While some entities have directed significant financial and human resources to protect themselves, creating such individual "cyber fortresses" provides only a thin veneer of protection to cyber threats. The American economy is a highly networked and interconnected system. The distributed nature of cybersecurity threats means that even individual strongholds are vulnerable to a wide variety of threat vectors. An impact to one component of the Nation's infrastructure systems may cause a ripple effect across a much greater part of that system—or even cause impacts to other critical infrastructure systems. Addressing these vulnerabilities requires a national level strategy to enhance the level of cybersecurity protections across a wide range of entities in the public and private sectors. At the same time, more specific approaches must be adopted to meet regional needs and requirements.

Proposal: Create a network of regionally distributed cybersecurity centers of excellence in strategic locations around the Nation to catalyze efforts to address local issues and participate in national initiatives. Locally, these centers would enhance the cybersecurity resilience of partners across specific regions, including state and local governments, federal and military partners, academic institutions, and private sector entities. By serving as a network to coordinate best practices, threat intelligence, mitigation strategies, R&D developments, and other critical resources, these centers would also serve the national interests. These centers would function as public-private partnerships, with participants drawn from government, industry, academia, and other key stakeholder groups. These centers would not compete with private sector cybersecurity service providers. Instead, the centers coordinate and augment regional cybersecurity efforts by working collaboratively with private and public sector entities. The National Institute of Standards and Technology (NIST) utilizes an analogous model throughout the centers that comprise its Manufacturing Extension Partnership (MEP) Network. The individual MEPs do not compete with industry, but instead facilitate access to resources and services within their geographic regions. The cybersecurity centers could (1) facilitate cybersecurity consulting services across designated critical infrastructure sectors specifically relevant to their regions, state and local government offices—including those administering state and local elections, small scale energy production facilities, healthcare facilities, and educational institutions; (2) enable access to unique and leading-edge facilities to conduct proactive cybersecurity R&D with regional partners and universities; and (3) provide training and education, including cyber certification and workforce reskilling activities, for a field that continues to evolve. These centers could also research and develop better communications methods for the general public. Even prior to the pandemic, the research community was moving toward less travel and more virtual interactions. In recent months, Zoom and other virtual engagement platforms have demonstrated both their importance and their cybersecurity vulnerabilities. These centers of excellence could play a role in researching ways for better, more reliable, and more secure remote interactions.

Proposed Funding: Each regional center would support about 150 personnel and require approximately $40M in funding. The expectation would be that each center would have an increasing amount of funding from regional partners, such that they could provide significant "self-funding" after 5 years and be self-sustaining after 10 (perhaps sooner).