MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Eighteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

August 28, 2023

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528

Dear Director Easterly:

I write to inquire about the Cybersecurity and Infrastructure Security Agency's (CISA) partnership with the Analysis & Resilience Center (ARC) for Systemic Risk and the Energy Threat Analysis Center (ETAC). As the Nation's Risk Manager, CISA is inherently an agency built on trust and collaboration. CISA has continued to evolve since its inception in 2018, but as it matures, the agency must also maintain the collaborative partnerships that have successfully managed critical infrastructure security and risk for years.

The vast majority of our nation's critical infrastructure is owned and operated by the private sector, including within the Financial Services Sector and the Energy Sector.[1] As such, in 2016, the Financial Services Information Sharing and Analysis Center (FS-ISAC) announced the establishment of the Financial Systemic Analysis & Resilience Center (FSARC), a public-private partnership with a mission to, "proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cyber security threats through focused operations and enhanced collaboration between participating firms, industry partners, and the U.S. Government."[2] The nation's eight largest banks pooled their resources and personnel into the FSARC to serve as a central operational collaboration hub to mitigate cyber risk and strengthen resilience in partnership with federal agencies including the Department of Homeland Security, Department of Treasury, and Federal Bureau of Investigation.

Following the success of the systemic risk frameworks and models created by the FSARC, the group expanded to the electricity subsector and formally rebranded in 2020 as the ARC.[3] The ARC similarly unified some of the nation's largest electric utilities with a common goal to mitigate systemic risk to the energy sector. At the same time, the ARC also announced intent to expand to other critical infrastructure

[1] *Partnerships and Collaboration*, CISA.GOV, https://www.cisa.gov/topics/partnerships-and-collaboration (last visited May 16, 2023).
[2] *FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC),* PRNEWSWIRE.COM, https://www.prnewswire.com/news-releases/fs-isac-announces-the-formation-of-the-financial-systemic-analysis--resilience-center-fsarc-300349678.html (last visited May 16, 2023).
[3] *Announcing the Formation of the Analysis & Resilience Center (ARC) for Systemic Risk*, BUSINESSWIRE.COM, https://www.businesswire.com/news/home/20201030005462/en/Announcing-the-Formation-of-the-Analysis-Resilience-Center-ARC-for-Systemic-Risk (last visited May 16, 2023).

sectors to ultimately develop a "unified, cross-sector coalition…to assess, prioritize, and mitigate risk."[4] In a continuation of the FSARC model, the ARC brought together a unique partnership where the financial services and energy industries could provide insight into real-world critical infrastructure equities and risk while also developing mitigation approaches, and the federal government could provide clearances and sensitive information as appropriate.

Despite ample engagement and participation in the ARC by the owners and operators of cross-sector critical infrastructure entities, and a history of engaging with the ARC since its inception, I understand that CISA may adopt a different sector-specific approach. I understand that at the end of 2022, the electricity members of the ARC left the organization to engage with the ETAC. Financial services sector stakeholders recently received written indication of CISA's intent to alter the ARC's facility clearance, although now CISA appears to have reconsidered and granted the facility clearance. The ARC model has proven effective and I encourage CISA to continue bolstering established partnerships. These partnerships will be crucial for the agency's broader public-private partnership strategy, at a time when threats from adversarial nations are unrelenting.

Given this lack of clarity around the future of CISA's relationships with these existing groups, particularly as the Joint Cyber Defense Collaborative (JCDC) matures, I request a briefing to address the following questions:

1. What, if any, role did CISA have in the establishment of the ETAC? How is CISA engaging with the ETAC?
2. Please describe any plans to absorb the ARC's risk register methodology and the ETAC as a "spoke" of CISA's JCDC.
3. Please describe any additional or possible plans to change CISA's relationship with the ARC, including absorbing it as a "spoke" of the JCDC.
4. How is CISA supporting cross-sector systemic risk and resilience efforts now that the agency is driving towards a sector-specific approach?
5. How does CISA intend to resource any expansion of the JCDC's "spokes" with the current Fiscal Year 2024 budget request?

I appreciate your prompt attention to this matter. I look forward to working with you to ensure U.S. critical infrastructure owners and operators maintain a strong relationship with federal partners like CISA. Please contact the committee at 202-226-8417 to schedule the briefing no later than September 28, 2023.

Sincerely,

ANDREW R. GARBARINO
Chairman
Subcommittee on Cybersecurity and
Infrastructure Protection

cc: ERIC SWALWELL
Ranking Member
Subcommittee on Cybersecurity and
Infrastructure Protection

[4] Id.