Ranking Member John Katko

SECURING SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE

If everything is critical, nothing is.

Most Americans had never heard of **Colonial Pipeline** until they felt the effects of the gas shortage caused by its shutdown. Most of us had also never heard of **SolarWinds**, despite the fact that its software was used by federal agencies and 80% of Fortune 500 companies. Nobody would dispute that these two events affected critical infrastructure after seeing the impact, but what if the cyber attacks targeted an amusement park or a shopping mall? Most Americans would not consider cyber attacks on those facilities to be nearly as critical, yet those too could be considered critical infrastructure. **The truth is, we don't have a truly comprehensive understanding of what is *actually* critical infrastructure.**

That is why **Rep. John Katko (R-NY)** has been working diligently to authorize a thoughtful, transparent, and stakeholder-involved process for identifying **systemically important critical infrastructure (SICI)** – to capture critical infrastructure whose disruption would have a debilitating effect on our national security, public health, or economic security. Katko has worked closely with **dozens of industry partners** to craft legislation that would not only accomplish this, but also direct the Cybersecurity and Infrastructure Security Agency (CISA) to prioritize **meaningful benefits** to SICI designees, **without any additional burden**. The current inefficient method of allocating services on a first-come, first-served basis is, by definition, not a risk-based allocation. We must change that to ensure that limited federal resources, especially at CISA, are focused on critical infrastructure facing the greatest risk.

Specifically, this legislation will:

- Authorize the CISA Director to **establish a transparent, stakeholder-driven process to designate systemically important critical infrastructure, or SICI.**
- **Bring in stakeholders from the very beginning** – requires CISA to consult with Sector Risk Management Agencies (SRMAs) and stakeholders in establishing a methodology and criteria for determining what critical infrastructure qualifies as SICI.
- **Provide CISA with clear guidance** and parameters for establishing the criteria for SICI.

- **Provide a pre-SICI determination feedback loop** – requires the Director to establish a Preliminary Determination Process that delays the designation for 30 days after the potential SICI owner or operator has been notified to provide the opportunity to share additional information with CISA.

- **Protection of information** – requires that information obtained by the Director pursuant to the process falls under CISA's robust information protection statutes, and be classified as appropriate.

- **Prioritize CISA services** – unlike previous initiatives, this bill requires that CISA provide SICI owners and operators with the option to take part in prioritized cybersecurity services, including:

    - **Front of the line access** for CISA's key cybersecurity programs, including technical assistance, and voluntary programs to continuously monitor and detect cybersecurity risks.

    - **Prioritized representation** in CISA's newly established Joint Cyber Defense Collaborative (JCDC).

    - **Prioritized applications** of SICI owners and operators for security clearances, as appropriate.

- **Require an initial assessment** – requires the Director, in coordination with SRMAs and stakeholders, to assess current CISA processes and capabilities for determining SICI, potential benefits of SICI designation, and opportunities for improved relationships between SICI owners and operators and the federal government.

- **Provide robust congressional oversight** – includes multiple opportunities for congressional oversight to ensure the authorities are being carried out as envisioned.