January 2022

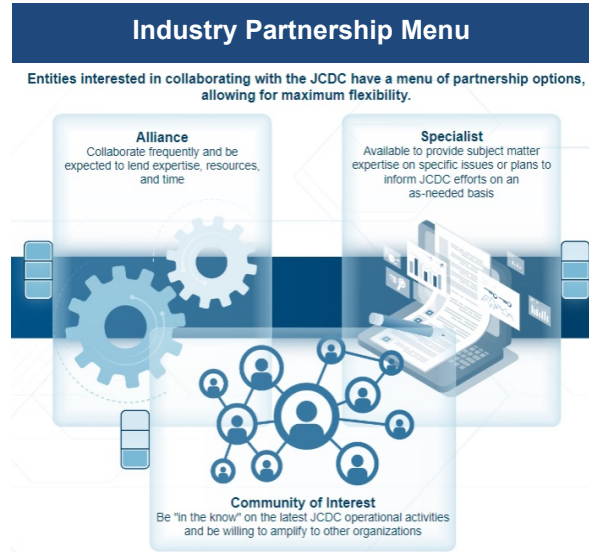## CHANGING THE CYBERSECURITY PARADIGM: A UNIFIED CYBER DEFENSE

The Joint Cyber Defense Collaborative (JCDC) leads integrated public-private sector cyber defense planning, cybersecurity information fusion, and dissemination of cyber defense guidance to reduce risk to critical infrastructure and National Critical Functions. JCDC addresses the global imperative for a more inclusive and operationally aligned community of cyber defenders to plan and exercise countermeasures against cybersecurity threats. This alignment strengthens our mutual resilience and ability to address immediate and impending cyber incidents. The JCDC model reflects the reality that no one entity can secure cyberspace alone and builds collective defense from the ground up. JCDC brings together a full spectrum of cyber defense partners—including U.S. federal as well as state, local, tribal, and territorial (SLTT) governments; private industry; and international governments and organizations.

Industry Partnership Menu

Entities interested in collaborating with the JCDC have a menu of partnership options, allowing for maximum flexibility.

Alliance
Collaborate frequently and be expected to lend expertise, resources, and time

Specialist
Available to provide subject matter expertise on specific issues or plans to inform JCDC efforts on an as-needed basis

Community of Interest
Be "in the know" on the latest JCDC operational activities and be willing to amplify to other organizations

JCDC partners have diverse and unique capabilities and expertise to reduce risk to the cyber ecosystem and to critical infrastructure. This diversity provides increased visibility and insight into the threat landscape and enables JCDC to develop plans and exercises against the most serious threats. Our private industry partners participate in JCDC at varying levels, as described in the menu above. Collaboration across JCDC partners results in support to—and actions across—an expansive set of cybersecurity stakeholders throughout the nation and the globe.

HOW WE WORK: PUBLIC-PRIVATE OPERATIONAL COLLABORATION

JCDC depends on the talent and expertise of its partners—including critical infrastructure companies—to execute the core functions below.

Collaborative Planning. JCDC coordinates operational cyber defense planning and execution. JCDC's joint cyber planning function includes deliberate and crisis action plans to address the most pressing cyber risks. This involves continuous measurement and improvement of the effectiveness of cyber defense planning and capabilities.

Information Fusion. JCDC drives collaborative public-private sector cybersecurity information sharing, fusion, and analysis. The JCDC operating model relies on regular analytic and data exchanges to enable common situational awareness and understanding. This information equips public and private sector partners to take risk-informed coordinated action for our collective defense.

Cybersecurity Guidance Production and Dissemination. JCDC develops and disseminates timely and actionable cybersecurity publications. Drawing upon the capabilities and expertise across JCDC partners, these publications provide cyber defenders with unified, coordinated, and richly informed guidance to prevent and mitigate cybersecurity threats and vulnerabilities.

For more information, contact us at cisa.jcdc@cisa.dhs.gov.

CISA | DEFEND TODAY, SECURE TOMORROW

cisa.gov · cisa.jcdc@cisa.dhs.gov · Linkedin.com/company/cisagov · @CISAgov | @cyber | @uscert_gov · Facebook.com/CISA · @cisagov