CISA Expands Cybersecurity Committee, Updates Baseline Security Goals

The US Cybersecurity and Infrastructure Security Agency (CISA) this week announced adding more experts to its Cybersecurity Advisory Committee (CSAC) and updating the baseline cybersecurity goals introduced last year.

CISA on Monday announced over a dozen new members of the CSAC, whose role is to advise the agency's director on policies and programs.

Members of the advisory committee include cybersecurity, tech, privacy, risk management and resilience experts from public and private sector organizations.

New members from the private sector include Dave DeWalt, CEO and founder of NightDragon; Brian Gragnolati, president and CEO of Atlantic Health System; Royal Hansen, VP of privacy, safety and security engineering at Google; Rahul Jalali, SVP and CIO at Union Pacific; Cathy Lanier, SVP and CSO at the NFL; Doug Levin, co-founder and national director at K12 Security Information eXchange; Kevin Tierney, VP and CSO at General Motors; and Alex Tosheff, SVP and CSO at VMware.

The new members who bring in expertise on the government side include Chris Inglis, former national cyber director; former representatives John Katko and Jim Langevin; Ciaran Martin, former CEO of the UK's National Cyber Security Centre; and Robert Scott, commissioner at the New Hampshire Department of Environmental Services.

“Chosen for their deep expertise in critical infrastructure, cybersecurity, and governance, these members will add important new perspectives to the CSAC’s work, particularly given this year’s additional focus on corporate cyber responsibility, technology product safety, and efforts to raise the cyber hygiene baseline of ‘target rich-cyber poor’ entities like hospitals, K-12 school districts, and water utilities,” said CISA Director Jen Easterly.

On Tuesday, CISA announced that it has updated the cross-sector cybersecurity performance goals (CPGs) unveiled last year.

The changes have been made based on feedback from stakeholders, who asked for the goals to be more easily traceable to the NIST Cybersecurity Framework. In response, CISA reorganized the goals to match the NIST framework.

The CPGs were created to help critical infrastructure and other organizations prioritize cybersecurity investments and address critical risks.

The CPGs focus on a prioritized subset of IT and OT security practices that can help reduce the likelihood and impact of risks and adversary techniques. In addition, they can serve as a benchmark for measuring and improving cybersecurity maturity.

Related: Digesting CISA’s Cross-Sector Cybersecurity Performance Goals

Related: CISA Seeks Public Opinion on Cloud Application Security Guidance

Related: CISA Program Warns Critical Infrastructure Organizations Vulnerable to Ransomware Attacks

https://www.securityweek.com/cisa-adds-experts-to-cybersecurity-committee-updates-baseline-security-goals/