THE
NATIONAL LAW REVIEW

DHS Issues Cybersecurity Strategy

Wednesday, May 16, 2018

The Department of Homeland Security ("DHS") released its cybersecurity strategy on May 15, 2018. The 35-page document sets forth a plan for managing cybersecurity risks through public and private sector collaboration. By 2023, DHS seeks to have "improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities." The strategy document is broken into five pillars: risk identification; vulnerability reduction; threat reduction; consequence mitigation; and enable cybersecurity outcomes. DHS assures that it "will maintain a leadership role, collaborating with other federal agencies, the private sector, and other stakeholders, across all of its cybersecurity mission areas to ensure that cybersecurity risks are effectively managed, critical networks are protected, vulnerabilities are mitigated, cyber threats are reduced and countered, incidents are responded to in a timely way, and the cyber ecosystem is more secure and resilient."

MURTHA CULLINA

Article By Murtha Cullina
Dena M. Castricone
Privacy and Cybersecurity Perspectives

Communications, Media & Internet
All Federal

Source URL: https://www.natlawreview.com/article/dhs-issues-cybersecurity-strategy