Cybersecurity and Risk Management

SAFETY Act Certification

Southern Company not only complies with government regulations and industry standards, including the Critical Infrastructure Protection cybersecurity reliability standards, but regularly goes above and beyond those mandatory requirements. As evidence of Southern Company's industry-leading commitment to cybersecurity, the U.S. Department of Homeland Security (DHS) has granted Certification for Southern Company's cybersecurity risk management program under the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act). Certification is the highest level of protection recognized under the SAFETY Act and is awarded after significant scrutiny of the covered technology along with evidence of proven effectiveness. This was the first such Certification granted by DHS for any company's internal cybersecurity risk management program.



Cybersecurity is a critical component of Southern Company's risk management program. We are committed to ensuring the security, reliability and resilience of our critical infrastructure against both physical and cyberattacks. Our strong approach to cybersecurity establishes oversight and accountability throughout the organization.

Southern Company's Board of Directors has established its Business Security and Resiliency (BSR) Committee that meets at every regular Board meeting and is charged with oversight of risks related to cybersecurity and operational resiliency. The BSR Committee includes Directors with an understanding of cyber issues and with high-level security clearances. Senior management also has high-level security clearances to ensure access to critical information, and the company participates in pilot programs with industry and government to share additional information and strengthen cybersecurity and business resiliency. Southern Company participates in the Electricity Subsector Coordinating Council (ESCC), which coordinates industry and federal government preparation for and response to potential national disasters and cyber-attacks. In addition, Southern Company Gas has representation on the Oil & Natural Gas Subsector Coordinating Council (ONGSCC).

Cybersecurity and Risk Management

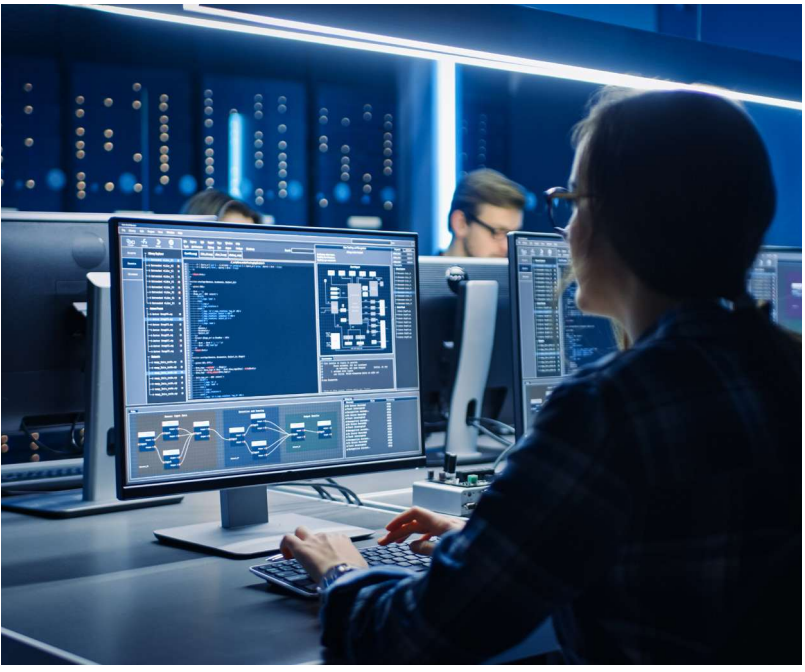
Cybersecurity Strategy

Southern Company protects its networks through a risk-based, "all threats" and "defense in depth" approach to identify, protect, detect, respond, and recover from cyber threats. Although many Southern Company networks are segmented, overall network security is a centralized "shared service" across the Southern Company system, led by the Technology Security Organization and the Chief Information Security Officer. Recognizing that no single technology, process or control can effectively prevent or mitigate all risks, Southern Company employs multiple technologies, processes, and controls, all working independently but as part of a cohesive strategy to minimize risk. This strategy is regularly tested through auditing, penetration testing, and other exercises designed to assess effectiveness.

Southern Company emphasizes both security and resiliency through business assurance and incident response plans designed to identify, evaluate, and remediate incidents when they occur. Southern Company utilizes a 24/7 Security Operations Center, which facilitates real-time situational awareness across the cyber-threat environment, and a robust Insider Threat Protection Program and Fusion Center that leverages cross-function information sharing to assess insider threat activity. Southern Company regularly reviews and updates its plans, policies, and technologies, and conducts regular training exercises and crisis management preparedness activities to test their effectiveness. These activities supplement the company's normal security awareness training programs for its employees, which are designed to educate and train employees about risks inherent to human interaction with information and operational technology.

In addition to the defense efforts within the company, helping our business partners maintain their security is essential to the overall protection of Southern Company. We host a six-week CAP training program that readies small businesses to seek Cybersecurity Maturity Model Certification (CMMC), a nationally and internationally recognized certification of expertise in lifecycle cybersecurity risk management required to do work with the U.S. government. Upon completion, each company is positioned to make its own determination of whether to earn their CMMC. The CAP training program was devised to combat the increased frequency of targeted and complex cyberattacks on businesses worldwide, against which small businesses struggle to defend themselves in particular. This initiative contributes greatly to Southern Company's overall level of cybersecurity.

Recognizing that no single technology, process or business control can effectively prevent or mitigate all risks, we employ multiple technologies, all working independently but as part of a cohesive strategy to minimize risk.



Intelligence Sharing Partnerships

Southern Company's cybersecurity program is increasingly leveraging intelligence sharing capabilities about emerging threats – within the energy industry, across other industries, with specialized vendors, and through public-private partnerships with government intelligence agencies. Southern Company's CEO chairs the Cybersecurity Advisory Committee, a board of industry and government leaders that advises the Director of the Cybersecurity & Infrastructure Security Agency (CISA) on the development, refinement, and implementation of recommendations, policies, programs, planning, and training pertaining to CISA's cybersecurity mission. By engaging with both the Electricity Information Sharing and Analysis Center (E-ISAC) and the Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC), Southern Company benefits from quality analysis and rapid sharing of security information across the energy sector. Such intelligence allows Southern Company to better detect and prevent emerging cyber threats before they materialize. Just as it tests its policies and plans internally, Southern Company also engages in external exercises such as GridEx to evaluate and address industry preparedness.