MARCH 6, 2017

NIST in the House – Empowering the Nation's Cybersecurity Standards-Maker To Head Off Increasing Cyber Threats to the Government and Its Contractors.

NIST in the House – Empowering the Nation's Cybersecurity Standards-Maker To Head Off Increasing Cyber Threats to the Government and Its Contractors by Christian Henel and Gunjan Talati.

The National Institute of Standards and Technology (NIST) recently received a vote of confidence in the U.S. House of Representatives that may increase its role and authority in defending the nation from cyber threats. On March 1, 2017, the House Committee on Science, Space and Technology approved the NIST Cybersecurity Framework, Assessment and Auditing Act of 2017 for submission to the broader House of Representatives. The Act proposes to amend the National Institute of Standards and Technology Act "to implement a framework, assessment, and audits for improving United States cybersecurity." If passed, the Act would empower NIST to assess and audit and report to Congress regarding federal agencies' cybersecurity defense capabilities. It also calls for NIST to submit to OMB guidance that would promote the incorporation of the NIST's sweeping framework of cybersecurity controls, best practices, and procedures into all federal agencies' existing cybersecurity practices for all federal agencies. Up until now, NIST has been toiling away on its framework while individual agencies picked and chose which aspects to incorporate into their cybersecurity regulations and contract clauses. The proposed law contemplates a more uniform approach.

Upgrading NIST from an advisory role to more of a regulator/auditor role could bring the federal government closer to effectively deploying uniform government-wide cybersecurity control standards. It might even reduce some of GAO's concerns, echoed in its most recent iteration of the high risk list – that agencies have been sluggish in addressing even the severe cybersecurity risks they face. From a contractor's perspective, uniformally implementing NIST will ideally provide predictability for contractors trying to understand in plain English the cybersecurity requirements that apply to their contracts. For now though, contractors must continue to navigate the patchwork of regulations across agencies that intermittently invoke NIST's publications but leave many questions about implementation and compliance unanswered.

Readers interested in additional background and information on NIST and federal cybersecurity requirements in general may want to consider attending the authors' presentation: "How to Prepare and Respond to a Data Breach" presented as part of Federal Publications Seminars' " Government Contracts

Week", May 9-12, 2017 in La Jolla, California.