HOUSE COMMITTEE ON
OVERSIGHT AND REFORM
CHAIRWOMAN **CAROLYN B. MALONEY**

Discussion Draft: Federal Information Security Modernization Act of 2022
Released by Chairwoman Carolyn B. Maloney and Ranking Member James Comer
House Committee on Oversight and Reform

The cyberthreat landscape has transformed dramatically since the Federal Information Security Management Act (FISMA) was enacted in 2002 and last updated in 2014. The onslaught of devastating cyberattacks like SolarWinds and the Microsoft Exchange Server hack, as well as vulnerabilities discovered in common Apache Log4j software, highlight the need to modernize FISMA with a clear, coordinated, whole-of-government approach to federal cybersecurity.

House Oversight and Reform Committee Chairwoman Carolyn B. Maloney and Ranking Member James Comer are working closely on the shared goal of FISMA reform. In drafting House companion legislation, the Committee has been coordinating with Chairman Gary Peters and Ranking Member Rob Portman of the Senate Committee on Homeland Security and Governmental Affairs, as well as the Administration's key cybersecurity leadership and industry stakeholders.

Chairwoman Maloney and Ranking Member Comer's discussion draft of the Federal Information System Modernization Act of 2022 would:

Clarify Federal Cybersecurity Roles for Improved Cooperation. Clearly assigns federal cybersecurity policy development and oversight responsibilities to the Office of Management and Budget (OMB), operational coordination responsibilities to the Cybersecurity and Infrastructure Security Agency (CISA), and overall cybersecurity strategy responsibilities to the National Cyber Director (NCD). Codifies the OMB Federal Chief Information Security Officer.

Advance a Risk-Based Cybersecurity Posture. Promotes cybersecurity modernization and next generation security principles like a risk-based paradigm, zero trust principles, endpoint detection and response, cloud migration, automation, penetration testing, and vulnerability disclosure programs. Replaces point-in-time assessments with ongoing and continuous risk assessments that will allow agencies to prioritize cybersecurity risks with accurate, real-time information about the agency's posture and threats.

Modernize and Streamline Reporting Requirements. Reduces the frequency of FISMA assessments while requiring continuous monitoring of systems, easing compliance burdens while enhancing security through the use of automation.

Expand Inventories and Information Sharing for Improved Security. Requires agencies to keep inventories of all internet-accessible information systems and assets, as well as all available software bills of materials, for improved situational awareness. Improves incident information sharing between agencies and oversight entities.

Promotes Shared Services and Agency Support. Requires CISA to expeditiously seek opportunities to remove barriers to agency cybersecurity efforts through shared services and technical assistance.