The Washington Post reports on a new report prepared for the Senate Homeland Security and Governmental Affairs Committee:

" The report draws on previous work by agency inspectors general and the Government Accountability Office to paint a broader picture of chronic dysfunction, citing repeated failures by federal officials to perform the unglamorous work of information security. That includes installing security patches, updating anti-virus software, communicating on secure networks and requiring strong passwords. A common password on federal systems, the report found, is "password."....The report levels particularly tough criticism at the Department of Homeland Security, which helps oversee cybersecurity at other federal agencies. The report concluded that the department had failed even to update essential software — "the basic security measure just about any American with a computer has performed."....Higher up the chain of command, agency directors are rarely held accountable for security failures, experts said, because it is often unclear who is responsible. No penalties are mandated by law."

Some examples from the report relevant to the energy sector:

"The Nuclear Regulatory Commission stored sensitive cybersecurity details for nuclear plants on an unprotected shared drive, making them more vulnerable to hackers and cyberthieves."

"Last January, hackers gained access to U.S. Army Corps of Engineers computers and downloaded an entire non-public database of information about the nation's 85,000 dams — including sensitive information about each dam's condition, the potential for fatalities if breached, location and nearest city."