United States Senate
COMMITTEE ON FINANCE
WASHINGTON, DC 20510–6200

February 11, 2022

Ms. Clare Martorana
Federal Chief Information Officer
Office of Management and Budget
725 17th St, N.W.
Washington, D.C. 20503

Dear Ms. Martorana:

We request you take immediate steps to secure the national Organ Procurement and Transplantation Network (OPTN) system from cyber-attacks. The Senate Finance Committee is currently conducting an investigation into the United States' organ transplant system and our congressional oversight includes, among other things, an examination of the security and technology issues surrounding the OPTN system. In light of our recent findings, we have no confidence in the security of this system.

In 1986, the U.S. Department of Health and Human Services (HHS), through the Health Resources and Services Administration (HRSA), awarded the first contract for the operation of the OPTN. Since that time, the OPTN has been operated by a government contractor known as the United Network for Organ Sharing (UNOS). UNOS is the only organization to ever hold the OPTN contract. As a result, since 1986, UNOS has solely operated the technology system used to maintain the national organ transplant waiting list and facilitate all organ procurement, matching, and allocation in the United States.

Our staff recently obtained a briefing from the U.S. Digital Service (USDS), which assessed the organ donation matching system in 2020. According to USDS, no one working for the federal government has ever examined the security of this system. Moreover, HHS, the agency responsible for the contract, has not imposed any cybersecurity requirements on UNOS, the contractor running the system. With no standards and no audits, the security of the system depends entirely on voluntary security investments made by the contractor, which USDS harshly criticized for its poor software engineering practices.

It is imperative that the Federal government secure the U.S. organ donation system. As mentioned above, UNOS is the sole operator of the system, and therefore maintains the entire waiting list for all organ transplant candidates in the United States. This means that any interruption in service—such as a ransomware attack, technical failure, or even inefficiency resulting in unnecessary delays—has the potential for lethal harm to patients across the country. Such a disruption would have a particular effect on Americans in the Medicare and Medicaid systems, particularly those suffering from kidney failure and receiving high cost dialysis treatments. To that end, we urge the Administration to ensure that the organ

donation system in the United States and the lives that depend on it are protected and secured from hackers.

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
Chairman
Committee on Finance

Charles E. Grassley
Member
Committee on Finance

CC: Xavier Becerra, Secretary of the Department of Health and Human Services
Jen Easterly, Director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency
Avril Haines, Director of National Intelligence