Statement for the Record

Michael J. LoSapio
Nominee for Director of the Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Before the
Committee on Homeland Security and Governmental Affairs
United States Senate

November 19, 2026

Chairman Paul, Ranking Member Peters, and distinguished Members of the Committee, I am honored to appear before you to discuss my nomination for Director of the Cybersecurity and Infrastructure Security Agency (CISA). I want to thank the President for nominating me and Secretary Mullin for his confidence in me. I also thank the Senators on this Committee and your staffs for your time throughout this process.

I want to recognize my family. I thank my parents, Barbara and Salvatore. Both taught me to show up every day, to work hard, and to put others before myself. I thank my wife, Lisa, for her love and patience through late-night incident calls for work, weekends at the firehouse, and now this process. And I thank our children, Michael, Mia, and Angelina, who are in school today and will be watching the highlights online tonight. They are a big part of why I care so much about getting this work right, and I hope they see that public service is worth the sacrifice it asks of a family. I am also grateful to my friends and to my colleagues at Palantir.

I have spent twenty years in technology and cybersecurity. I began as a systems administrator at Seton Hall University and Stevens Institute of Technology, and since then there are few layers of the technology stack I have not built, run, or defended, from websites and email servers to supercomputing clusters, high-speed research networks, virtual private networks, and production software. I have also managed crises. At New York University ahead of Hurricane Sandy in 2012, our team powered down data centers, migrated critical services to our disaster recovery site, and kept essential communications running for students and staff, and as fire chief of the Warren Township Fire Department, I led our response to emergencies in my township handling rescues, fire responses and coordinating critical resource requests at the county, state and national level. In 2013, I joined Palantir Technologies as a founding engineer for its cloud hosted environment, and after roles at Oscar Insurance and MemSQL, I returned in 2017 to join its security engineering team. As the team's lead, I directed infrastructure and network security for hundreds of thousands of cloud assets and grew the engineering team sixfold. Along the way, I have hardened cloud environments, computers, and phones and worked through standards such as NIST SP 800-53 and FedRAMP, turning compliance requirements into real security for our customers and our company.

Since September 2024, I have served as Palantir's Chief Information Security Officer, where I lead a large team across our alerting, detection, and response; identity and access management; infrastructure; endpoint; and network security teams, protecting highly sensitive data platforms at global scale. That work has taught me that security is a team effort, that decisions often have to be made quickly and with incomplete information, and that the trust you need in a crisis has to be

built well before the crisis arrives. I hold a bachelor's degree in computer science from Seton Hall University and an MBA from New York University, along with several professional security certifications.

Outside of work, I have served the public as a volunteer firefighter since 1999 and an EMT since 2001, and I rode with a rescue squad for almost ten years. I am a life member of the Mount Bethel Volunteer Fire Company in Warren Township, New Jersey. Twenty-five years in the fire service taught me how to lead under pressure, coordinate across jurisdictions when a crisis hits, and show up when people need help most. If confirmed, this would be my first role in federal service, and I would be honored to bring those lessons to it.

The threats to our Nation's networks and infrastructure are serious and growing. Nation-state actors have positioned themselves inside the systems that deliver our power, water, and communications, and criminal groups use ransomware against hospitals, schools, and small towns that cannot afford to be offline.

Congress established CISA as America's cyber defense agency and the national coordinator for critical infrastructure security and resilience. My view of the job is simple: CISA should make the Nation harder to attack and faster to recover, and it should do so by earning the trust of the people who own and operate our infrastructure. If confirmed, I will focus on four lines of effort.

The first is defending federal agencies, where CISA has direct operational responsibilities. That means better visibility across agency networks, faster detection and response, and timely remediation of known exploited vulnerabilities, measured by results rather than paperwork.

The second is serving as a trusted operational partner to critical infrastructure owners and operators and to state, local, tribal, and territorial governments. CISA must deliver timely and actionable information, maintain a strong regional presence, support operational collaboration through the Joint Cyber Defense Collaborative, and continue its work in physical security and emergency communications.

The third is reducing risk at the source. The Known Exploited Vulnerabilities catalog gives defenders a clear signal about what to fix first, and working with technology manufacturers to make products secure by design and by default shifts the burden away from hospitals, water utilities, and small towns that would otherwise fix flaws after the fact.

The fourth is the workforce and stewardship of public resources. I will work to recruit and keep talented people, give them clear priorities, and make sure every dollar Congress provides is spent with discipline and tied to measurable results. I also thank this Committee for its leadership in establishing and strengthening CISA, and Acting Director Nick Andersen and the men and women of CISA for their work every day.

Cybersecurity, like firefighting, is a team effort. CISA succeeds only in close collaboration with its partners in government and industry. I look forward to a productive and transparent partnership with this Committee.

I thank the Committee for considering my nomination and look forward to your questions.