UNIVERSITY OF MARYLAND

OFFICE OF THE PRESIDENT

Main Administration Building
College Park, Maryland 20742
301.405.5803 TEL 301.314.9560 FAX

SENATE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION
Testimony of Dr. Wallace D. Loh
President, University of Maryland
March 26, 2014

My name is Wallace Loh and I am the President of the University of Maryland. From its beginnings as a small, land-grant institution to its current status as a major presence in higher education, the University of Maryland has a long and distinguished history of excellence and innovation, evidenced by being #38 in the 2013 Academic Ranking of World Universities.

I am grateful for this opportunity to discuss an issue that is not only important to the higher education community but to all of us who participate in online activities on a daily basis. As the state's flagship institution, the University of Maryland has 37,000 students, 12 colleges and schools, 9000 faculty and staff, and an annual $1.7 billion operation budget. To safeguard such a large and complex operation, we recently doubled the number of our IT security engineers and analysts as well as our investment in top-end security tools. However, as our recent data breach reveals, more remains to be done.

On February 18, 2014, the University of Maryland was the victim of a sophisticated computer security attack that exposed records containing personal information of faculty, staff, students and affiliated personnel from the College Park and Shady Grove campuses. Fortunately, no financial, academic, health or contact (phone and address) information was compromised, but we are not taking any chances. I have ordered five years of credit protection services at no cost to every person affected by this breach. This is above and beyond the protection measures taken by other organizations and institutions, and so far nearly 30,000 persons affected by the breach have registered, which is also well ahead of projections. In addition, all sensitive records in the breached database that are no longer required have been removed.

As evidence of our efforts, the University of Maryland IT security staff, working with the U.S. Secret Service, the FBI, and the campus police, mitigated another intrusion which occurred on Saturday, March 15, 2014. There was no public release of any information and no damage to the institution, except for the release of personal data of one senior university official.

Our experience highlights a serious and growing threat. In fact, in the past decade, some 20 large universities across the country have also reported major data breaches. Fortunately, there are steps that can be taken to minimize our risk and vulnerability.

Over the past month, the University of Maryland has handled the situation in a deliberate and thorough manner, working with computer forensic investigators to determine how our sophisticated, multi-layered security defenses were bypassed, to track down the perpetrators, and most importantly to ensure there is no repeat of these intrusions. The steps we are taking now should serve as both a warning and a model for other institutions.

First, many university databases were created years ago when the environment for cyber threats was different. Consequently, they need to be explored, updated and secured. A comprehensive review of all personal information across all databases is underway, which has already led to the removal of all sensitive records in the breached database that are no longer required. Second, to maintain protection, universities should perform penetration tests of security defense on an ongoing basis to seal any possible technological gaps. At the moment, we are evaluating cyber security consulting firms that can assist with this process. Finally, there must be an appropriate balance between centralized (University-operated) versus decentralized (unit-operated) IT systems. Technical fixes must be reflected in policy changes to ensure that safeguards at central and local levels are equally robust and tightly coordinated. This includes examining national cybersecurity policies, procedures and best practices. The University of Maryland is performing each of these steps and recommends that other universities follow suit. And while such changes may be pricey, being proactive in safeguarding sensitive information is worth the investment.

To execute this threefold mission, I have formed an 18-member Task Force on Cybersecurity. The Task Force includes experts from our campus, including members from our Maryland Cybersecurity Center. It also includes students since their perspective is unique and essential. The first meeting of the Task Force took place March 12 and I have charged them to complete an investigation and submit recommendations to me by June 12. The Task Force has the full support of my office and the resources it needs to complete its task. I will take all necessary actions based on the Task Force's recommendations and the results of the forensic analysis now underway.

Concurrently, the University IT staff with the support of outside consultants are working virtually non-stop to protect better the vast information systems in our network that are accessible to students, faculty, staff and others. In the past month, they have identified and closed the pathways utilized in the February 18, 2014, breach and the incursion on March 15, 2014, changed the passwords for all databases and applications, and conducted an initial audit to detect vulnerabilities in individual websites within web hosting environments. Plans have also been accelerated to migrate web hosting to a more secure environment.

Equally important, it is not enough to rely on others to defend against cyber threats. Each of us must do our part and take reasonable steps to ensure our own information security. Therefore, the University of Maryland will also present a series of identity theft seminars to our students, faculty, staff and alumni. These seminars, which will also be recorded and made available online for viewing at a later time, will feature Jeff Karberg from the Maryland Attorney General's Identity Theft Unit.

It is clear that there is no impregnable barrier against every cyber-attack. There is an arms race between hackers playing offense and universities playing defense. Nonetheless, as the threat evolves, so can we. It will require higher investments in cyber security and greater diligence on our part, but as we become more adept at defense, we will inevitably create a good offense, and cyber criminals will have to be the ones who are worried.

Thank you.

Wallace D. Loh