Testimony of Michael J. Astrue for the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies of the House Committee on Homeland Security

September 11, 2013

Chairman Meehan, Ranking Member Clarke, and Members of the Subcommittee, no day is more fitting than 9/11 for us to cherish and safeguard our liberties as Americans.

I testify today only as a former official. A quarter-century ago, I briefly was the White House's Privacy Act officer. I then served as General Counsel of the U.S. Department of Health & Human Services and as Commissioner of Social Security for Presidents Bush and Obama. As Commissioner, I also served as a Trustee of the Medicare Trust Fund.

Some history helps us understand why we needed to have this hearing. Infighting and paralysis marked the first year of the effort to construct the federal health exchanges, including what is called the "data hub." Administrator Berwick claimed that he could not find the money to build the system, and he criticized Congress for not specifically appropriating money for it. He also criticized Secretary Sebelius for refusing to release money from the ACA discretionary fund.

Berwick pressed other agencies to pay for the exchange, even though such payments would violate appropriations restrictions. When development started in earnest after

Berwick's departure, CMS struggled to meet its deadline. CMS's failures and delays have been common knowledge within the Administration, yet HHS was never candid with states as they were choosing either to build their own exchanges or to use the CMS exchanges.

From 2007-2013, I led the overhaul and expansion of Social Security's suite of electronic services. I personally reviewed every major system before beta testing, and extensive beta testing often revealed the need for delays to make changes. We involved not only random focus groups, but also advocates for various people, such as victims of domestic violence.

We need to be very concerned about protecting the privacy of the data stored in these types of systems, which I believe are not adequately protected. The defense offered by the Center for Democracy & Technology and others—that the CMS systems are just a "routing tool," not a repository—is either untrue or problematic. CMS needs to store data to create forensic trails necessary to track security breaches; failure to establish forensic trails would create a serious issue under the Federal Information Security Management Act of 2002.

We need to know whether unauthorized changes of insurance could leave Americans unexpectedly uninsured. We need to know how CMS will define and respond to breaches—I know how important that is because I suffered through OPM's inept response when my federal financial records were breached two years ago. We need to know why many of the people who will deal with the public are just being hired now, and being hired without background checks. A rigorous authentication

process may result in as many as two million people who will need to interact with CMS contractors when they fail to access the system—is CMS ready for that workload or are they going to sacrifice service or authentication? Greater transparency about these issues would improve the quality of the exchanges—*and* increase public confidence in the system.

Both SSA and the IRS formally appealed to OMB that the exchanges would violate the Privacy Act, violations which potentially carry criminal penalties. OMB eventually denied that appeal, but in my view HHS will be violating the Privacy Act on a massive scale by allowing people to make insurance decisions for other adult family members without their written consent. This feature of the system may well allow domestic abusers to track down their victims.

An August 2, 2013 Inspector General report revealed that the CMS schedule has slipped so badly that mandatory security findings are scheduled for *the day before implementation*. With no room for adequate beta testing and revisions, HHS's claim that it will be ready to make security findings on its September 30 deadline is a fiction designed to preserve the larger fiction that the exchanges will be ready for uninsured Americans.

Before I conclude, I urge President Obama and Congress to scrutinize the performance of HHS Inspector General Levinson. Relying only on interviews and documents, his August 2, 2013 report on the exchanges contained *less than five pages of analysis*. His staff did not even *try* to use the beta version of the system.

HHS cannot have it both ways. If the exchanges can function on October 1, by July of this year there must have been a beta version. However, the Inspector General did not inspect the beta version, and meekly noted that CMS *withheld security documents*. He ignored the vulnerabilities of a system that transmits, largely through the so-called "cloud," sensitive personal information to CMS contractors and private insurers. He ignored the privacy issues, the security issues, and the issues associated with poorly screened and trained contractors. He did *not* assess usability, performance measures, governance or contingency plans. With HHS's expanded role in health care, Americans need an Inspector General who is a watchdog, not a lapdog.

Congress is bitterly divided about the Affordable Care Act, but there should be common ground. Whether or not you support an individual mandate, you can embrace the principle that no one should be forced to sacrifice privacy in order to comply with that mandate. To the best of my knowledge, work on systems that would comply with the Privacy Act stopped in early 2013 after OMB brushed aside the Privacy Act appeals of SSA and the IRS. A system respecting the Privacy Act would probably take an additional 6-18 months to develop.

President Obama has delayed other parts of the Affordable Care Act. Vulnerable Americans without lobbyists deserve the same respect and deference given to the business community. You should support a moratorium on the exchanges until HHS secrecy ends, and until we know whether uninsured Americans, will be forced to pay—along with their premiums—the high price of their privacy.

Thank you.