UNITED STATE SENATE COMMITTEE ON
HOMELAND SECURITY
& GOVERNMENTAL AFFAIRS
SUBCOMMITTEE ON REGULATORY AFFAIRS
AND FEDERAL MANAGEMENT

SENATOR JAMES LANKFORD, CHAIRMAN | SENATOR HEIDI HEITKAMP, RANKING MEMBER

November 17, 2015

Opening Statement of Senator James Lankford

Homeland Security and Governmental Affairs Subcommittee on Regulatory Affairs and Federal Management Hearing titled:

"ONGOING CHALLENGES AT THE U.S. SECRET SERVICE AND THEIR GOVERNMENT-WIDE IMPLICATIONS"

Good afternoon. I'd like to thank Chairman Perry for his willingness to hold this important joint hearing with our Subcommittee. I'm hopeful that our efforts here today will shed light on how one of our top law enforcement agencies failed to protect sensitive personal information housed in internal databases.

At the outset, it is important to acknowledge the essential security role that the Secret Service fills, and its ongoing dedication to our country. However, the recent history of high profile and embarrassing scandals at the Service and the latest DHS Inspector General findings of wrongdoing cannot be swept under the rug. The IG's investigation reveals that unauthorized database searches of protected information began during a House Oversight and Government Reform hearing in March of this year. In the days that followed, many at the Secret Service continued to misuse their authority to access the sensitive employment history of Chairman Jason Chaffetz. The IG's report noted 60 instances of unauthorized access to the database by 45 Secret Service employees that violated the Privacy Act as well as internal and DHS policies.

The report also noted that 18 senior Secret Service executives failed to stop the unauthorized access or inform Director Clancy about the unauthorized accesses. In fairness, the report does reflect that one Special Agent instructed her subordinates to cease accessing the database. On its face, such widespread violations of our law and the public's trust are deeply disturbing. The IG did not question those involved if this was the only time they have inappropriately used the database. In the internet age, everyone is concerned about the possibility that personal information could be stolen or misused.

Our elite law enforcement agencies are not above the law and those responsible must face appropriate consequences. But to me, there is also a much bigger issue for us to examine. These days millions of Americans' personal data is stored not just on databases at the Secret Service, but across many government agencies. A GAO report released earlier this year on the government's federal information security showed alarming findings. From 2009 to 2014 the number of information security incidents involving personally identifiable information reported

by federal agencies has more than doubled. GAO has stated that many agencies have largely failed to fully implement the hundreds of recommendations previously made to remedy security control vulnerabilities.

These security weaknesses continue to exist in the protection of the significant personal data of millions of Americans housed by the IRS, HHS, the VA and other agencies. Just this month, the Social Security Administration's Office of the Inspector General released a report showing that the Social Security Administration paid monetary awards to 50 employees who were previously discovered to have accessed the personal information of others without authorization. Fifty federal employees who accessed the personal information of others, without authorization and yet incredibly in the end they were rewarded despite breaking the law. In another troublesome example, the Senate Homeland Security Committee received testimony this year that a whistleblower was retaliated against for shedding light on inadequate suicide-prevention practices at a VA hospital.

This whistleblower learned that VA employees illegally and improperly accessed his private medical records after he brought to light the shameful behavior occurring at the VA hospital where he served. So it's not just the Secret Service that has employees who illegally accessed private information, this behavior has occurred across government. The question is how do we fix this problem so that Americans believe that government will protect their information and not use it to for nefarious means. I am hopeful today we can take a step forward to address this issue.

I'd like to thank Director Clancy, Inspector General Roth, and Mr. Willemssen for their testimony today. I look forward to examining these challenges with each of you.