United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

"Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards"
Senator Joseph I. Lieberman
Subcommittee on
Oversight of Government Management, the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs
March 26, 2007

I want to thank Chairman Akaka for convening this hearing today which will provide the Committee an opportunity to finally shine much needed light on the REAL ID Act of 2005 by reviewing the rules that have been proposed for this program in an open forum.

Earlier this month, the Department of Homeland Security (DHS) issued a Notice of Proposed Rulemaking (NPRM) implementing the REAL ID Act. The NPRM, which took the Department almost two years to issue, does little to alleviate the concerns that I, and many of my colleagues, expressed two years ago when the REAL ID Act was attached to an emergency spending bill and forced through Congress without debate or substantive consideration.

The proposed regulations will cost approximately $23 billion according to the Office of Management and Budget, will bring Department of Motor Vehicle offices across the United States to a stand still, and may actually jeopardize security. We should not cause undue burden to the American public if security can be achieved in a more sensible way.

I remain fully committed to increasing the security of drivers' licenses and identification cards, which should be a top priority for this country. However, I am concerned, as I was two years ago, that the REAL ID Act impedes rather than facilitates the achievement of that goal.

In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act to implement the recommendations of the 9/11 Commission. Senators McCain, Collins and I worked together closely to produce reasonable, bi-partisan solutions based on the Commissioners' recommendations. One recommendation required the federal government to set national standards for the issuance of drivers' licenses and identification cards. This was based on the Commission's finding that many of the 9/11 hijackers obtained U.S. identification documents, some by fraud. We took this recommendation seriously and carefully crafted provisions - with input from both sides of the aisle and all interested constituencies - to increase the security and reliability of drivers' licenses and identification cards. Our provisions were endorsed by state and local governments, the Administration, and a range of immigration, privacy, and civil liberties advocacy groups.

Regrettably, the REAL ID Act repealed those balanced provisions and replaced them with an unworkable, burdensome mandate. I opposed the REAL ID Act because I believed it imposed such unrealistic requirements that without substantial time and resources, it would not be implemented, making the nation less safe as a result. If the original Intelligence Reform Act provisions had not been repealed, states would be well on their way to securing drivers' licenses today. Instead, DHS was saddled with implementing such a controversial and complex law that the Department took two years to issue regulations.

After reviewing the NPRM, I remain concerned about REAL ID implementation because it does not appear that DHS has addressed many of the problems and concerns identified two years ago.

First, the REAL ID Act requires states to verify all documents used to obtain a REAL ID, such as a birth certificate. To do so, states must rely on a series of electronic systems and federal databases. Yet some of these databases don't exist or are incomplete. Others are known to contain inaccurate data. One of the most egregious examples is the Electronic Verification of Vital Events (EVVE) system, which was developed by the National Association for Public Health Statistics and Information Systems (NAPHSIS) to provide a single interface for verification of birth and death records. EVVE is currently in pilot form, and only seven states have access. Even if all fifty states had access to the EVVE system, it would not allow for credible electronic verification of birth and death records because the database will not contain records from all the states. NAPHSIS issued a report in January 2006 stating that the EVVE system could take as long as seven years to be fully operational. The report specifically noted that the system must be implemented nationwide before it will be beneficial for REAL ID. A valid, verified birth certificate is at the heart of REAL ID, yet the timelines for these two programs are completely incompatible.

In addition to the EVVE system, REAL ID relies upon a non-existent State Department system to verify U.S. passports and the DHS Systemic Alienation Verification for Entitlements (SAVE) system, which is notorious for containing erroneous, incomplete, or outdated information. Moreover, even though the success of REAL ID depends on these systems, there is no requirement in the REAL ID Act or in the NPRM that the federal agencies provide these systems in a timely or accurate manner. The states will be left holding the bag if the federal government fails to deliver.

I am also troubled by the incomplete nature of the proposed regulations. There is virtually no guidance in the NPRM regarding what type of electronic system will be used to share information between states. This detail is critical to understanding the security and privacy vulnerabilities that may be created by REAL ID. Assistant Secretary Barth has said that the Department of Transportation's Commercial Driver's License Information System (CDLIS) will likely be the model used for REAL ID. CDLIS allows information on licensed commercial drivers to be shared between states on a limited basis -- commonly referred to as a "pointer system." However, the NPRM does not specify a pointer system will be used for REAL ID, leaving the realization of a de facto national database as a distinct possibility under the regulations.

Given the inevitable incompleteness and inaccuracies of the REAL ID databases, it is shocking to me that the NPRM does not call for a redress system. This is not a function that can be left to the states because REAL ID and the information it relies upon are bigger than the individual states. What happens if one state passes erroneous information about an individual to another state? Chances are there will be cases where both states claim it's the responsibility of the other state to adjudicate the complaint. Where does an individual turn if a state DMV and a federal agency cannot agree on who should correct an incomplete record? DHS needs to mandate a redress process and make it clear where that responsibility lies to ensure errors and oversights are resolved promptly.

Also notably absent from the NPRM is a requirement to encrypt the data held electronically on the actual ID card. Without encryption it will be substantially easier to steal critical personal information, making all Americans more vulnerable to identity theft. Equipment capable of reading the Machine Readable Zone on the back of most drivers' licenses is readily available. If we're going to spend billions of dollars enhancing the security of the rest of the identification system, why leave this gaping hole?

DHS has chosen to pass the responsibility for privacy protection to the states. This is inherently problematic because REAL ID requires states, and more importantly the individual citizen, to provide and share additional personal information in the name of security. Because REAL ID is a federal mandate, the federal government has an obligation to ensure the law is implemented appropriately and that information shared under REAL ID is secure. States deserve some flexibility in implementing REAL ID as they are the ones who understand the drivers' licensing process. However, given the security implications of widespread identity theft, the federal government cannot remain silent on this issue.

Most troubling is that DHS has elected to hide behind what is not said in the REAL ID Act as a means to avoid addressing privacy. The NPRM states, "DHS has sought to address these privacy concerns within the limits of its authority under the Act…. The Act does not include language authorizing DHS to prescribe privacy requirements for state-controlled databases or data exchange necessary to implement the Act." The concept that federal agencies need explicit Congressional authorization to protect Americans' privacy is just plain wrong. In fact, our government is obligated to ensure that programs and regulations do not unduly jeopardize an individual's right to privacy.

Privacy is inherently tied to security. Secretary Chertoff made this argument earlier this month when he told the Northern Virginia Technology Council that "Security and privacy are very much the same type of value. I don't think they're mutually exclusive, they're mutually reinforced." As Secretary Chertoff argued, executed correctly, better standards for drivers' license issuance will strengthen privacy safeguards and help prevent identity theft. However, we must remember that if this process is executed poorly, it will have the opposite effect.

Finally, it should be noted that states across the country are moving to opt out of REAL ID. Because of the program's structure, it is only as strong as its weakest member. If we create a system so onerous that it precludes full participation, any security benefit is lost.

While I regret the repeal of the common sense provisions in the Intelligence Reform Act, which I believe has made identification security much more difficult, I am committed to ensuring this job is done right. We must find a way to make the driver's license a trusted document, and the road the Department is now on is not the way. Secure identification is at the very heart of our homeland security. I strongly encourage the Department to consider the concerns expressed by Congress and others in formulation of the regulations. And I look forward to working with Chairman Akaka, Senator Collins, the Department of Homeland Security, and others to solve this critical and complex problem.

-30-