

REAL ID Basic Overview
March 2007

Privacy & Security Concerns

- Mandating that each state **create a database** without statutory limitations on what information can be placed in the database (i.e., in a person's record), including source documents [§202(d)(13)]
- Mandating that each state give every other state "electronic access" to the database (i.e., people's records) with the ostensible but unstated limited purpose of ensuring that no driver holds more than one license and without a limitation on creating a **central ID database** [§202(d)(12)]
- Mandating that each state give every other state "electronic access" to the database (i.e., people's records) and without statutory limitations on **what information can be shared** between states and for *what purposes*; *who else* (e.g., other state agencies, federal agencies, third-parties) can access the databases and for *what purposes* [§202(d)(12)]
- Moving states toward digitally **copying** all highly-sensitive **source documents** (e.g., birth certificate, Social Security Card, passport, utility bill) and housing them in a database; and without statutory limitations on *who* can access them and for *what purposes* [§202(d)(2)]
- Mandating that states "**verify**" **source documents** without statutory limitations related to the collection and sharing of personal information, by *whom* and for *what purposes* [§202(c)(3)(A)]
- Mandating that each card have Machine Readable Technology (MRT); and without statutory limitations on *what* information is stored in the Machine Readable Zone (**MRZ**), *who* can "skim" information from the MRZ (e.g., state agencies, federal agencies, third-parties) and for *what purposes*; and without statutory security requirements such as encryption [§202(b)(9)]
- No statutory limitations on "**official purpose**" [§202(a)(1)]
- No statutory clarity on whether driver's license/ID card **number** will be **unique** within a state or across the nation [§202(b)(4)]

Secure Issuance Measures CDT Agrees With

- Standardizing which source documents, regarded as generally reliable, may be used to get a driver's license or ID card
- Verifying the authenticity of the source documents and the accuracy of the information contained therein
- Requiring minimum security features for the cards themselves to deter tampering and counterfeiting
- Security of the physical locations where cards are made and supplies stored to deter outsider fraud
- Security measures to deter insider fraud such as employee background checks and strict access controls to information and supplies