



**ASSISTANT SECRETARY FOR POLICY  
STEWART A. BAKER**

Stewart A. Baker was appointed by President Bush to be Assistant Secretary for Policy for the Department of Homeland Security and confirmed by the U.S. Senate on October 7, 2005.

Prior to his appointment and confirmation as Assistant Secretary, Stewart A. Baker served as General Counsel of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (2004-2005), where he headed the drafting team for the Commission's report. He also served as General Counsel of the National Security Agency (1992-1994) and Deputy General Counsel of the Department of Education (1979-1981). When not engaged in government service, he was an associate and partner at the Washington, D.C., law firm of Steptoe & Johnson LLP. Earlier, Mr. Baker served as a law clerk to John Paul Stevens, US Supreme Court (1977-78), Frank M. Coffin, US Court of Appeals, First Circuit (1976-77), and (as an intern law clerk) Shirley M. Hufstедler, US Court of Appeals, Ninth Circuit (1975).

Mr. Baker has been named to numerous US government, private, and international bodies dealing with national security, technology, and related topics, including: President's Export Council Subcommittee on Export Administration (2003-present); Commerce Department's Industry Trade Advisory Committee on Information and Communications Technologies, Services, and Electronic Commerce (2003-present); Markle Foundation Task Force on National Security in the Information Age (2002-2004); Defense Science Board's Task Force on Information Warfare (1995-1996; and 1999-2001); Federal Trade Commission's Advisory Committee on Online Access and Security (2000); President's Export Council Subcommittee on Encryption (1998-2001); Free Trade of the Americas Experts Committee on Electronic Commerce (1998-2003); UNCITRAL Group of Experts on Digital Signatures (1997-2001); OECD Group of Experts on Cryptography Policy (1995-1997); International Telecommunication Union Experts Group on Authentication (1999); American Bar Association Standing Committee on Law and National Security (1998-2005); International Chamber of Commerce Working Party on Digital Authentication (1996-1998); International Chamber of Commerce Group of Experts on Electronic Commerce (1996-2005). Mr. Baker was awarded the Defense Medal for Meritorious Civilian Service in 1994.

**From:** Baker, Stewart [mailto:Stewart.Baker@dhs.gov]

**Sent:** Wednesday, January 14, 2009 7:28 AM

**To:** Mike Delph

**Cc:** Cissna, Francis

**Subject:** Answers to Questions

- 1. When an employer enters into the E-Verify agreement with DHS, the biz community claims they give up some of their 4<sup>th</sup> AM rights under the US Const. True/False and explanation.**

False. Whether an employer is an E-Verify participant or not, they would still be subject to any audits or investigations allowable under the law. As a condition to agreeing to become an E-Verify participant, employers agree to permit review of records by the Department of Homeland Security and the Social Security Administration, but only after a reasonable notice. Employers who sign the MOU are not consenting to a search, and even if signing the MOU could be (mistakenly) construed as such consent, any such consent can be withdrawn at the time DHS or SSA requests access.

- 2. When an employer enters into the E-Verify agreement with DHS, the biz community says that it puts them in a discrimination paradox. True/false and explanation.**

False. The rules for E-Verify were developed to ensure that employers CANNOT engage in illegal discrimination. As a participant in E-Verify, employers are required to verify all newly hired employees, both U.S. citizens and non-citizens. Employers may not verify selectively, and must verify all new hires while participating in the program. The program may not be used to prescreen applicants for employment, go back and check employees hired before the company signed the MOU, or re-verify employees who have temporary work authorization. If an employee receives a Tentative Nonconfirmation (TNC) during the verification process, the employer must provide them the opportunity to contest the TNC and resolve the discrepancy in their record. Under the law, the employee must also be allowed to continue working and the employer may not take any adverse action against the employee while resolution of a TNC is pending. An employer may only terminate an employee when employment is not authorized (SSA Final Confirmation, DHS Final Confirmation, or DHS No Show), and the E-Verify statute expressly protects employers who act in good faith reliance on the results produced by the E-Verify system from any liability resulting from those actions. Employers who do not use the E-Verify with any intent to discriminate against workers on the basis of national origin or other protected status would qualify for that protection.