in the Systems or such databases may not be transferred to or shared with any Federal, State, or local government officials for any purpose other than preventing unauthorized workers from obtaining employment.

''(K) PROTECTION AGAINST UNLAWFUL INTERCEPTION AND DATA BREACHES.—The Commissioner of Social Security and the Secretary shall protect against unauthorized disclosure of the information transferred between employers, the Commissioner, and the Secretary and between the Commissioner and the Secretary by requiring that all information transmitted be encrypted.

''(L) ROBUST COMPUTER SYSTEM AND SOFTWARE SECURITY.—The Commissioner of Social Security and the Secretary shall employ robust, state-of-the-art computer system and software security to prevent hacking of the System or the databases employed.

''(M) SYSTEM SECURITY TESTING.—

''(i) REQUIREMENT FOR TESTING.—The Commissioner of Social Security and the Secretary shall require periodic stress testing of the System to determine if the System contains any vulnerabilities to data loss or theft or improper use of data. Such testing shall occur not less often than prior to each phase-in expansion of the System.

''(ii) REQUIREMENT TO REPAIR VULNERABILITIES.—Any computer vulnerabilities identified under clause (i) or through any other process shall be resolved prior to initial implementation or any subsequent expansion of the System.

''(iii) REQUIREMENT TO UPDATE.—The Secretary shall regularly update the System to ensure that the data protections in the System remains consistent with the state-of-the-art for databases of similarly sensitive personally identifiable information.

''(N) PROHIBITION OF UNLAWFUL ACCESSING AND OBTAINING OF INFORMATION.—

''(i) IMPROPER ACCESS.—It shall be unlawful for any individual, other than the government employees authorized in this subsection, to intentionally and knowingly access the System or the databases utilized to verify identity or employment authorization for the System for any purpose other than verifying identity or employment authorization or modifying the System pursuant to law or regulation. Any individual who unlawfully accesses the System or the databases or shall be fined no less than $1,000 for each individual whose file was compromised or sentenced to less than 6 months imprisonment for each individual whose file was compromised.

''(ii) IDENTITY THEFT.—It shall be unlawful for any individual, other than the government employees authorized in this subsection, to intentionally and knowingly obtain the information concerning an individual stored in the System or the databases utilized to verify identity or employment authorization for the System for any purpose other than verifying identity or employment authorization or modifying the System pursuant to law or regulation. Any individual who unlawfully obtains such information and uses it to commit identity theft for financial gain or to evade security or to assist another in gaining financially or evading security, shall be fined no less than $10,000 for each individual whose information was obtained and misappropriated sentenced to not less than 1 year of imprisonment for each individual whose information was obtained and misappropriated.

''(O) OFFICE OF EMPLOYEE PRIVACY.—

''(i) ESTABLISHMENT.—The Commissioner of Social Security and the Secretary shall establish a joint Office of Employee Privacy that shall be empowered to protect the rights of employees subject to verification under the System.

''(ii) AUTHORITY TO INVESTIGATE.—The Office of Employee Privacy shall investigate alleged privacy violations concerning failure of the Commissioner or the Secretary to satisfy the requirements of subparagraphs (H) through (Q) of this paragraph and any data breaches that may occur pursuant to the implementation and operation of the System.

''(iii) AUTHORITY TO ISSUE SUBPOENAS.—The head of the Office of Employee Privacy may issue subpoenas for a document or a person to facilitate an investigation.

''(iv) ANNUAL REPORT TO CONGRESS.—The head of the Office of Employee Privacy shall submit to Congress an annual report concerning the operation of the System.

''(v) ANNUAL REPORT ON INCORRECT NOTICES.—The head of the Office of Employee Privacy shall, at least annually, study and issue findings concerning the most common causes of the incorrect issuance of nonconfirmation notices under the System. Such report shall include recommendations for preventing such incorrect notices.

''(vi) AVAILABILITY OF REPORTS.—The head of the Office of Employee Privacy shall make available to the public any report issued by the Office concerning findings of an investigation conducted by the Office.

''(vii) REQUIREMENT FOR HOTLINE.—The head of the Office of Employee Privacy shall establish a fully staffed 24-hour hotline to receive inquiries by employees concerning tentative nonconfirmations and final nonconfirmations and shall identify for employees, at the time of inquiry, the particularity data that resulted in the issuance of a nonconfirmation notice under the System.

''(viii) CERTIFICATION BY GAO.—The Secretary may not implement the System or any subsequent expansion or phase-in of the System unless the Comptroller General of the United States certifies that the Office of Employee Privacy has hired sufficient employees to answer employee inquiries and respond in real time concerning the particular data that resulted in the issuance of a nonconfirmation notice.

''(ix) TRAINING IN PRIVACY PROTECTION.—The head of the Office of Employee Privacy shall train any employee of the Social Security Administration or the Department of Homeland Security who implements or operates the System concerning the importance of and means of utilizing best practices for protecting employee privacy while utilizing and operating the System.

''(P) AUDITS OF DATA ACCURACY.—The Commissioner of Social Security and the Secretary shall randomly audit a substantial percentage of both citizens and work-eligible noncitizens files utilized to verify identity and authorization for the System each year to determine accuracy rates and shall require correction of errors in a timely fashion.

''(Q) EMPLOYEE RIGHT TO REVIEW SYSTEM INFORMATION AND APPEAL ERRONEOUS NONCONFIRMATIONS.—Any employee who contests a tentative nonconfirmation notice or final nonconfirmation notice may review and challenge the accuracy of the data elements and information in the System that resulted in the issuance of the nonconfirmation notice. Such a challenge may include the ability to submit additional information or appeal any final nonconfirmation notice to the Office of Employee Privacy. The head of the Office of Employee Privacy shall review any such information submitted pursuant to such a challenge and issue a response and decision concerning the appeal within 7 days of the filing of such a challenge.''.

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Mr. CORNYN. Mr. President, I ask unanimous consent that the Committee on Homeland Security and Governmental Affairs be authorized to meet on Friday, March 31, 2006, at 10 a.m. to consider the nomination of Uttam Dhillon to be Director of the Office of Counternarcotics Enforcement at the U.S. Department of Homeland Security and, immediately following the hearing, to consider the nomination of Mark D. Acton to be Commissioner of the Postal Rate Commission.

The PRESIDING OFFICER. Without objection it is so ordered.

COMMITTEE ON THE JUDICIARY

Mr. CORNYN. Mr. President, I ask unanimous consent that the Senate Committee on the Judiciary be authorized to meet to conduct a hearing on An Examination of the Call to Censure the President on Friday, March 31, 2006, at 9:30 a.m. in Room 226 of the Dirksen Senate Office Building.

Witness List

Panel I: Robert F. Turner, Associate Director, Center for National Security Law, University of Virginia, Charlottesville, VA; Bruce Fein, Partner, Fein & Fein, Washington, DC; Lee Casey, Partner, Baker & Hostetler, Washington, DC; John Dean, White House Counsel to President Richard Nixon, Author, Worse than Watergate; John Schmidt, Partner, Mayer Brown Rowe Maw LLP, Chicago, IL.

The PRESIDING OFFICER. Without objection, it is so ordered.

PRIVILEGE OF THE FLOOR

Mr. CORNYN. Mr. President, I ask unanimous consent that the privilege of the floor be granted for the duration of the immigration debate to Susannah Prucka, a member of my staff on the Subcommittee on Immigration, Border Security and Citizenship.

The PRESIDING OFFICER. Without objection, it is so ordered.

EXECUTIVE SESSION

EXECUTIVE CALENDAR

Mr. FRIST. Mr. President, I ask unanimous consent that the Senate immediately proceed to executive session to consider the following nominations on today's Executive Calendar: Calendar Nos. 599, 603, and 604. I further ask unanimous consent that the nominations be confirmed en bloc, the motions to reconsider be laid upon the table, the President be immediately notified of the Senate's action, and the Senate then return to legislative session.

The PRESIDING OFFICER. Without objection, it is so ordered.

The nominations considered and confirmed en bloc are as follows: