I

107TH CONGRESS
2D SESSION

H. R. 5671

To promote the secure sharing of information and communications within the Department of Homeland Security.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 16, 2002

Mr. JOHN introduced the following bill; which was referred to the Committee on Government Reform

---

A BILL

To promote the secure sharing of information and communications within the Department of Homeland Security.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Information Security Act.''

SEC. 2. FINDINGS AND PURPOSES.

(a) FINDINGS.—Congress finds the following:

(1) The securing of information will play a vital role in rapidly transforming the Department of Homeland Security into a cohesive organization.

(2) Without the ability to share information securely and to collaborate securely, the Department of Homeland Security cannot carry out its mission to strengthen homeland security.

(b) PURPOSE.—The purpose of this Act is to require the Department of Homeland Security to fund, implement, and maintain the enhanced security infrastructure necessary for sensitive information to be securely stored, transmitted, and disseminated within the Department.

SEC. 3. MANAGED DIGITAL CERTIFICATES.

The Chief Information Officer and the Under Secretary for Management of the Department of Homeland Security shall work with the heads of key Department of Homeland Security agencies, including the United States Customs Office and the United States Office of Immigration and Naturalization Services, to implement managed digital certificate-based security projects and to issue to Department employees managed digital certificates, that—

(1) provide standards-based e-mail encryption and digital signature capabilities;

(2) permit interoperability with the Federal Bridge and other Government public key infrastructure systems and applications;

(3) demonstrate proven scalability;

(4) support multiple platforms; and

(5) include automated, secure key, and certificate management.

SEC. 4. DEFINITIONS.

In this Act:

(1) DIGITAL CERTIFICATE.—The term ''digital certificate'' means a digital identifier that authenticates an individual or an appliance on a computer network.

(2) MANAGED DIGITAL CERTIFICATE.—The term ''managed digital certificate'' means a digital certificate supported by a technology infrastructure that manages the certificate's life-cycle from creation, issuance, revision, and cancellation.

(3) MANAGED DIGITAL CERTIFICATE-BASED SECURITY.—The term ''managed digital certificate-based security'' means security services predicated upon the use of managed digital certificates.

(4) FEDERAL BRIDGE.—The term ''Federal Bridge'' means a clearinghouse that interprets and manages digital certificates so different Government departments and agencies can securely interoperate.

○