KEY ISSUE: PRIVACY, SURVEILLANCE & CYBERSECURITY

OBJECTIVE: Restore the Constitutional privacy rights of library users and the civil liberties of all Americans lost to overbroad and inadequately “checked and balanced” statutes, including the: USA PATRIOT Act, Foreign Intelligence Surveillance Act and Electronic Communications Privacy Act.

PERSPECTIVE: For decades, librarians have defended the public’s Fourth Amendment privacy rights against government attempts to obtain patrons’ borrowing and web browsing records without a warrant. The American Library Association (ALA) works with and through broad bipartisan coalitions of major public interest groups, think tanks and private sector companies to achieve both liberty and security, without sacrificing one for the other.

LEGISLATIVE ACTION: ALA urges Members of the 115th Congress to:

♦ **PASS** the *Email Privacy Act* (H.R.387) to reform the *Electronic Communications Privacy Act* of 1986 to afford emails, texts, tweets, cloud-stored files and all other modern electronic communications full Fourth Amendment protection upon their creation by requiring that authorities first secure a judicially-authorized search warrant to acquire their content, just as the law has long required for personal papers and similar tangible records.

♦ **OPPOSE** S. 1297 to make *Sec. 702 of the Foreign Intelligence Surveillance Act* (FISA) permanent and expand surveillance activities under it in favor reforming FISA to: preclude the warrant-less “back door” search of citizens’ phone and internet communications facilitated by the targeting of non-US citizens domestically or abroad; dramatically limit the true “incidental” collection and dissemination of communications by “US persons;” and regularly provide the public with non-classified data on the nature and scope of Section 702’s use.

♦ **REJECT** any legislation that would compel, or authorize courts to compel, the designer of any encryption system or technology to build “back doors” or other vulnerabilities into their products to intentionally permit the defeat or breach of such a system or technology; and

♦ **DEVELOP** clear statutory protocols requiring any government agency that becomes aware of a vulnerability in widely used software or hardware to assist the producer of affected products to eliminate that vulnerability for the public’s and the economy’s protection.