

SECTION-BY-SECTION SUMMARY OF THE CYBER CRIME PROTECTION SECURITY ACT

Section 1 - Short Title.

The bill is entitled the “*Cyber Crime Protection Security Act of 2012*”.

Section 2 – Organized Criminal Activity in Connection with Unauthorized Access to Personally Identifiable Information

Section 1 amends 18 U.S.C. § 1961(1) to add violations of the Computer Fraud and Abuse Act to the definition of racketeering activity. This change would increase certain penalties, and make it easier for the Government to prosecute certain organized criminal groups who engage in computer network attacks.

Section 3 – Penalties for Fraud and Related Activity in Connection with Computers

Section 2 amends title 18, United States Code, section 1030(c) to streamline and enhance the penalty structure under section 1030.

Section 4–Trafficking in passwords

Section 3 expands the scope of the offense for trafficking in passwords under title 18, United States Code, section 1030(a)(6) to include passwords used to access a protected government or non-government computer, and to include any other means of unauthorized access to a government computer.

Section 5–Conspiracy and attempted computer fraud offenses

Section 4 amends title 18, United States Code, section 1030(b) to clarify that both conspiracy and attempt to commit a computer hacking offense are subject to the same penalties as completed, substantive offenses.

Section 6 – Criminal and civil forfeiture for fraud and related activity in connection with computers

Section 5 amends title 18, United States Code, sections § 1030(i) and (j) to: (1) create a civil forfeiture provision, (2) provide the procedures governing civil forfeiture, (3) clarify that the proceeds that may be forfeited under section 1030 are gross proceeds, as opposed to net proceeds, and (4) allow for the forfeiture of real property used to facilitate section 1030 offenses.

Section 7– Damage to Critical Infrastructure Computers

Section 6 adds a new criminal provision to title 18 specifically making it a felony to damage a computer that manages or controls national defense, national security, transportation, public health and safety, or other critical infrastructure systems or information. Violations are subject to a fine and/or imprisonment of up to 20 years.

Section 8 -- Limitations on Actions Involving Unauthorized Use

Section 8 amends the definition of “exceeds authorized access” in title 18, United States Code, section 1030, to exclude conduct that only involves violating a terms of use agreement, or other contractual agreement governing the use of a non-government computer. This provision is intended to address concerns that relatively innocuous conduct, such as violating a terms of use agreement involving a privately owned computer, could result in criminal prosecution under section 1030.

Section 8 – Limitations on Certain Actions Involving Unauthorized Use

Section 7 amends title 18, United States Code, section 1030(a)(2) to clarify the types of criminal prosecutions that may be brought under the Computer Fraud and Abuse Act for conduct that involves intentionally exceeding authorized access to a computer. The provision requires that criminal offenses under the exceeds authorized access prong must involve either, information valued at more than \$5,000; sensitive or private information -- including trade secrets or confidential business information; classified information; or information obtained from a government computer. The purpose of the amendment is to prevent criminal prosecutions based upon innocuous conduct, such as violations a terms of use agreement.