Updated Administration Proposal:
Law Enforcement Provisions

Section-by-Section Explanations

SEC. 101. Prosecuting Organized Crime Groups That Utilize Cyber Attacks

This change adds offenses under the Computer Fraud and Abuse Act (18 U.S.C. § 1030) to the list of racketeering activities in the Racketeering Influenced and Corrupt Organizations Act (RICO at 18 U.S.C. § 1961(1)). This change would increase certain penalties and make it easier to prosecute organized criminal groups that engage in computer network and similar attacks.

SEC. 102. Deterring the Development and Sale of Computer and Cell Phone Spying Devices

These provisions provide additional tools to address violations of 18 U.S.C. § 2512, which criminalizes the sale, distribution, and advertising of surreptitious interception devices. First, it adds section 2512 to the list of money laundering predicates found in 18 U.S.C. § 1956, enabling appropriate charges for defendants who engage in money laundering to conceal profits from the sale of surreptitious interception devices. Second, it expands section 2513 (which already provides for the forfeiture of surreptitious interception devices themselves) to allow for the criminal and civil forfeiture of proceeds from the sale of surreptitious interception devices and any property used to facilitate the crime. This amendment to 2513 uses language found in forfeiture provisions in other title 18 sections.

SEC. 103. Modernizing the Computer Fraud and Abuse Act

Section 103 would update and clarify several provisions of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) to enhance its effectiveness against attacks on computers and computer networks, including those by insiders. Specifically, 18 U.S.C. § 1030(a)(2)(A) would reach any person who intentionally accesses a protected computer without authorization and thereby obtains information from such computer. 18 U.S.C. § 1030(a)(2)(B) creates a separate offense for a person who intentionally exceeds authorized access to a protected computer and thereby obtains information from such computer. To come within this provision, the value of the information obtained must exceed $5,000, the offense must be committed in furtherance of a felony, or the protected computer must be owned or operated by or on behalf of a governmental entity. In addition, this proposal amends the definition of "exceeds authorized access" (18 U.S.C. § 1030(e)(6)) to include accessing a computer with authorization and using such access to obtain or alter information in such computer for a purpose that the accesser knows is not authorized by the computer owner.

The amendments also alter section 1030(a)(6) to enable the prosecution of the sale of a "means of access" such as a botnet. The provision amends the mental state that the government is required to prove from "intent to defraud" (which applies only to financial motivations) to "willfully" so that the provision will apply to other types of wrongdoing perpetrated using botnets.

This proposal also:

- Clarifies that both conspiracy and attempt to commit a computer hacking offense are subject to the same penalties as completed, substantive offenses.
- Condenses and clarifies the penalty provisions (18 U.S.C. §1030(c)) by removing references to subsequent convictions in favor of setting a maximum sentence for each offense – in general, the maximum would be the number of years currently designated for a second offense.
- Enhances the criminal penalties for several of the offenses under 18 U.S.C. §1030.
- Amends 18 U.S.C. § 1030(i) and (j) to (1) create a civil forfeiture provision, (2) designate Chapter 46 of Title 18 as providing the procedures governing civil forfeiture, (3) clarify that the "proceeds" forfeitable under section 1030 are gross proceeds, as opposed to net proceeds, and (4) allow forfeiture of real property used to facilitate offenses under section 1030 in appropriate cases.

SEC. 104. Ensuring Authority for Courts to Shut Down Botnets

This proposal would empower courts to issue injunctions to disrupt or shut down botnets. It adds 18 U.S.C. § 1030 to the list of offenses for which injunctive relief may be sought under 18 U.S.C. § 1345, upon a showing that the criminal conduct would affect 100 or more protected computers during a 1-year period. The amendment would also create liability protection for companies that act in compliance with court orders under the section, and allow courts to order reimbursement where companies incur reasonably necessary compliance costs.