Section by Section

LAW ENFORCEMENT PROVISIONS RELATED TO COMPUTER SECURITY

Part 1: The Computer Fraud and Abuse Act (CFAA, at 18 U.S.C. §1030) establishes a series of criminal offenses for attacks on the confidentiality, integrity, and availability of computers. While these crimes apply to the computers and networks that run our critical infrastructure, there is no mandatory minimum penalty for such offenses. While it is reasonable to believe that courts would impose appropriately deterrent prison terms if an attack severely debilitates a critical infrastructure system, it is possible that courts might not impose adequate penalties for attacks that cause less disruption (or none at all in the case of an attempt that is thwarted before it is completed). This proposal would therefore create a mandatory minimum penalty for these sorts of attacks. The language is patterned on the very successful mandatory sentence for identity theft offenses, 18 U.S.C. § 1028A (Aggravated Identity Theft).

Part 2: This proposal would clarify several existing criminal offenses relating to attacks on computers and computer networks and enhance their penalties. Specifically, the proposal:

- Adds offenses under the CFAA to the list of 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 certain organized criminal groups who use computer network attacks.
- 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.
- 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.
- Expands the scope of the offense for trafficking in passwords (18 U.S.C. §1030(a)(6)), for example to cover passwords for access to any protected computer, not just government computers or where the trafficking affects interstate or foreign commerce.
- Enhances the criminal penalties for several of the offenses under 18 U.S.C. §1030.