

PAN 1.3b National Cybercrime Victim Assistance and Recovery Center

Staff Introduction to Proposal. This proposal establishes a federally supported nonprofit National Cybercrime Victim Assistance and Recovery Center to serve as a nationwide cybercrime reporting and recovery program to support individuals and small businesses, and an Office of Cybercrime Recovery at the Department of Justice to administer funding to the Center and coordinate with other US government efforts. Whereas existing crime reporting efforts at the Federal Bureau of Investigation and the Federal Trade Commission focus on gathering reports for law enforcement, the Center would focus on connecting individuals and small businesses victimized by technology-enabled fraud, theft, extortion, stalking, domestic/partner abuse, and other forms of cybercrime with informational resources and experts to aid in victim recovery. The Center and Office would (1) provide resources and technical help to victims; (2) provide onsite and offsite training and technical assistance to law enforcement and criminal justice professionals; and (3) compile, publish, and disseminate an annual summary and analysis of research related to cybercrime to provide law enforcement, policymakers, and the public with more accurate information on cybercrime trends.

Legend.

This proposal largely follows the statutory template and language of the Juvenile Justice and Delinquency Prevention Act of 1974 which created the Office of Juvenile Justice and Delinquency Prevention within the Department of Justice; the Missing Children’s Assistance Act (Division II of the Continuing Appropriations for FY1985) which established a national resource center and clearinghouse (managed by the private, non-profit National Center for Missing and Exploited Children via an annual grant); and the Victims of Crime Act of 1984 which established the Office for Victims of Crime.

A BILL

To Establish a Resource Center for Small Business and Individual Victims of Cybercrime

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

SEC. 1. SHORT TITLE.

This Act may be cited as the “National Cybercrime Victim Assistance and Recovery Center Act”.

SEC. 2 NATIONAL CYBERCRIME VICTIM ASSISTANCE AND RECOVERY CENTER.

(a) ESTABLISHMENT.—There is established within the Department of Justice the Office for Cybercrime Recovery (hereinafter referred to in this act as “Office”).

(b) APPOINTMENT OF DIRECTOR; AUTHORITY; RESTRICTIONS.—Not later than 90 days after the date of the enactment of this Act, the Office shall be headed by a Director

(referred to in this Act as the “Director”), who shall be appointed by the President from among individuals who have had experience in combating cybercrime, cybercrime victim assistance, cybersecurity incident response and recovery, or a related field. The Director shall report to the Attorney General through the Assistant Attorney General for the Office of Justice Programs and shall have final authority for all grants, cooperative agreements, and contracts awarded by the Office. The Director shall not engage in any employment other than that of serving as the Director, nor shall the Director hold any office in, or act in any capacity for, any organization, agency, or institution with which the Office makes any contract or other agreement under this Act.

(c) DUTIES AND FUNCTIONS.—The Director shall—

- (1) Administer funds made available by section 3 of this Act;
- (2) Establish programs in accordance with subsection (d) on terms and conditions determined by the Director to be consistent with that subsection;
- (3) Provide for the furnishing of technical indicators and trends on tactics and techniques used in cybercrime incidents that may be derived from the work of the national center established under subsection (d) and in accordance with subsection (e) to the Cybersecurity and Infrastructure Security Agency and other federal departments and agencies as determined by the Director;
- (4) Prepare an annual comprehensive plan for facilitating cooperation and coordination among all U.S. government departments and agencies with responsibilities related to providing recovery assistance for individual or small business victims of cybercrime;
- (5) Make such arrangements as may be necessary and appropriate to facilitate effective coordination among all federally funded programs related to providing recovery assistance for individual or small business victims of cybercrime; and
- (6) Such other functions as the Attorney General may delegate related to providing recovery assistance for individual or small business victims of cybercrime.

(d) ESTABLISHING A NATIONAL CYBERCRIME VICTIM ASSISTANCE AND RECOVERY CENTER.—The Director, either by making grants to or entering into contracts with public agencies or nonprofit private agencies, shall—

- (1) Establish and operate a national cybercrime victim assistance and recovery center (referred to in this act as the “Center”) by which individuals and small businesses request information and technical assistance, which may include providing referrals to third-party computer service providers, counseling, and criminal justice advocacy, necessary to—
 - (A) Identify and contact the appropriate law enforcement, regulatory, and other authorities for the purposes of reporting cybercrime incidents;
 - (B) Recover from cybercrime incidents that compromise data, confidentiality, integrity, and availability of information and information systems; and
 - (C) Protect against future cybercrime incidents;

- (2) Establish and operate a national resource center and clearinghouse to—
 - (A) Provide technical assistance to State, local, Tribal, and territorial governments and public and private nonprofit agencies in support of victim assistance and recovery services to small businesses and individuals impacted by cybercrime incidents;
 - (B) Assist in coordination of public and private programs which provide technical assistance to victims of cybercrime; and
 - (C) Disseminate information about innovative and model cybercrime victims’ assistance programs, services, and legislation;

- (3) Compile, publish, and disseminate an annual summary and analysis of research related to cybercrime, including completed and ongoing research; research conducted in non-profit, academic, private sector, and other non-governmental institutions; and Federal, State, and local demonstration projects relating to cybercrime with particular emphasis on—
 - (A) Effective models of local, State, and Federal coordination and cooperation in responding to cybercrime;
 - (B) Effective programs designed to promote community awareness of the problem of cybercrime;
 - (C) Effective programs to prevent cybercrime; and
 - (D) Effective program models which provide treatment, counseling, or other aid to individuals or owners and/or employees of small businesses who have been the victims of cybercrime;

- (4) Cooperate with and provide technical assistance as resources of the Center allow to States, units of local government, and other public and private organizations or international agencies involved in activities related to assisting individual and small business victims of cybercrime;

(5) Provide information deemed appropriate by the Director to the President, the Congress, Federal, State, local, Tribal, and territorial law enforcement, and other federal agencies, the private sector, and the general public on cybercrime; and

(6) Perform other functions, as directed by the Director or the Attorney General.

(e) PROTECTION OF INFORMATION.—No officer or employee of the Federal Government or agent of the Federal Government may, without the consent of the individual, entity, agency, or other person who contacts the Center,—

(1) Use any report or request that is furnished exclusively for the purposes of technical assistance or victim services under the provisions of this section for any purpose other than the purposes for which the submission is furnished and, after ensuring that any identifiable information has been removed, for statistical purposes;

(2) Make any publication or media transmittal of the data developed during the activities outlined in subsection (d) that permits information concerning individual entities or individual incidents to be reasonably inferred by either direct or indirect means; or

(3) Permit anyone other than an employee, agent, or contractor of the Center to examine an individual report or request for assistance described in subsection (d).

(f) LIMITATIONS.—Nothing contained in this Act shall be construed to—

(1) Grant to the Office, Director, or Center, any law enforcement power or responsibility; or

(2) Expand, narrow, or modify in any form, a crime or the elements of any criminal offense.

(g) CYBERCRIME DESCRIBED.—For the purposes of providing assistance to victims as described in this section and collecting statistical information pertaining to such incidents, cybercrime shall have the meaning as it is described in the Computer Fraud and Abuse Act (18 U.S. Code §1030), and further includes—

(1) technology-enabled fraud and identity theft;

(2) compromise of electronic system or service availability, to include denial of service attacks and sabotage;

(3) compromise of confidential personal or business electronic communications or information systems;

(4) Ransomware and extortion enabled through compromising the confidentiality, integrity, and availability of information and information systems;

(5) Abusive content sent or shared through digital information systems;

(6) Unauthorized access to or compromise of information stored through electronic means, to include photos, correspondence, and other data;

(7) Technology-enabled harassment and stalking;

(8) Technology-based domestic or intimate partner abuse and technology-enabled coercive control; and

(9) Such other incidents as the Director determines appropriate.

(g) DEFINITIONS.—In this section:

(1) CLEARINGHOUSE.—The term “clearinghouse” includes relevant databases and experts who could help identify and document best practices with respect to victim and recovery services, and then connect victims of cybercrime to such information.

(2) FEDERAL ENTITY.—The term “Federal entity” means a department or agency of the United States or any component of such department or agency.

(3) INFORMATION SYSTEM.—The term “information system” has the meaning given such term in section 3502 of title 44, United States Code and includes:

(A) industrial control systems, such as supervisory control and data acquisition systems;

(B) distributed control systems; and

(C) programmable logic controllers.

(4) SMALL BUSINESS.—The term “small business” means an entity considered to be a small business concern under section 3 of the Small Business Act (15 U.S.C. 632).

SEC. 3. AUTHORIZATION OF APPROPRIATIONS.—To carry out the provisions of this Act, there are authorized to be appropriated \$39,006,165 for fiscal year 2022, and such sums as may be necessary for fiscal years 2023, 2024, and 2025.

SEC. 4. CONFORMING AMENDMENT.—Subchapter II of chapter 53 of title 5, United States Code, is amended in section 5315 by inserting after “Administrator, Office of Juvenile Justice and Delinquency Prevention.” the following:

“Director, Office for Cybercrime Recovery.”.