

ATTORNEY GENERAL ADMINISTRATIVE DIRECTIVE 2005-2

ESTABLISHING AN OFFICIAL STATEWIDE POLICY REQUIRING ADOPTION OF THE ATTORNEY GENERAL'S COMPUTER CRIME TASK FORCE

WHEREAS, it is necessary and appropriate for the State of New Jersey to maximize its criminal justice resources and expertise by developing state-of-the-art technology and cutting-edge training to enhance our ability to combat the constantly evolving manifestations of high technology and computer crime;

WHEREAS, there are numerous units within the Department of Law and Public Safety performing criminal law enforcement functions under the auspices of the Attorney General with experience and expertise in dealing with issues related to high technology and computer crime, including the Computer Analysis and Technology Unit (CATU) of the Division of Criminal Justice, the Division of State Police Digital Technology Investigations Unit (DTIU) and the Division of State Police Cyber Crimes Unit (CCU);

WHEREAS, the Attorney General is empowered to implement administrative strategies and organizational planning to enhance and assure the highest level of proficiency in the performance of law enforcement functions to safeguard the public, and is required, consistent with N.J.S.A. 52: 178-4, to ensure that the Department of Law and Public Safety conducts its work in an efficient manner so as to avoid and/ or eliminate overlapping and duplicative functions;

WHEREAS, in light of the diverse resources situated within the Department of Law and Public Safety which are currently utilized to perform functions related

to the detection, investigation and prosecution of high technology and computer crime, it is prudent to establish a more integrated, cohesive and centralized unit to streamline law enforcement efforts to protect against the insidious illicit activities of cyber criminals who utilize technology to victimize the citizens of New Jersey;

NOW, THEREFORE, I, Peter C. Harvey, Attorney General of the State of New Jersey, do hereby **DIRECT** the following:

1. Establishment of the Attorney General's Computer Crime Task Force.

There is created in the Department of Law and Public Safety the Attorney General's Computer Crime Task Force (AGCCTF), which consists of the Computer Analysis and Technology Unit (CATU) of the Division of Criminal Justice, the Division of State Police Digital Technology Investigations Unit (DTIU) and the Division of State Police Cyber Crimes Unit (CCU). The AGCCTF shall be located at the Hamilton Technology Complex facility at 1200 Negron Drive in Hamilton, New Jersey, which consolidation of resources and personnel at the same location as the New Jersey Regional Computer Forensics Laboratory (NJRCFL) will streamline law enforcement efforts to investigate and prosecute cyber criminals.

2. Supervision. The Attorney General's New Jersey Computer Crime

Task Force shall operate under the cooperative partnership of the Supervising Deputy Attorney General (SDAG) of CATU in the Division of Criminal Justice (DCJ) and the Bureau Chief of the Computer Crimes and High Technology Surveillance Bureau of the Division of State Police (DSP Bureau Chief).

3. Operational and Administrative Protocols. The SDAG and the DSP Bureau Chief shall have joint authority to establish operational and administrative protocols, and to implement best management practices for the Task Force. The Task Force protocols and best practices shall include, but not be limited to, the following components:

(a) Review and maintain all applicable Standing Operating Procedures regarding intelligence gathering, investigative protocols, case screening, assignment and tracking, coordination of press releases and other administrative matters;

(b) Comply with all established standards for legal, technical and forensic protocols concerning the seizure, handling, storage and analysis of all forms of evidence; and

(c) Maintain a master case management system to monitor all investigative matters handled by the Task Force from inception through prosecution to prevent duplication of efforts or conflict.

The cooperative partner agency supervisors shall take all reasonable steps

to ensure that these procedures are coordinated and adequate.

4. Legal Affairs Division. (a) The SDAG shall be the head of the Legal Affairs Division, which is comprised of Deputy Attorneys General of the Division of Criminal Justice. The Legal Affairs Division has the right of first refusal for all cases initiated or investigated by the AGCCTF, except for those cases originating from a county prosecutor's office or a municipal police department. Based on legal requirements and implications, the Legal Affairs Division provides oversight and guidance on investigative techniques to be used on Task Force cases. Cases that are handled by the Legal Affairs Division shall follow established DCJ protocol for the review and approval of criminal cases. The SDAG shall make the final prosecutorial determination in consultation with the DSP Bureau Chief regarding which cases shall be brought by AGCCTF and the manner in which these cases are presented. All Legal Affairs Division DA'sG must confer with the SDAG before approving the use of new investigative techniques to determine the appropriate legal implications and requirements of such technology. In cases referred to a county prosecutor, or in cases originating from a county prosecutor's office, that county prosecutor shall provide all legal advice and services for those cases. The Legal Affairs Division may provide legal support to the county as needed.

(b) The SDAG is responsible for establishing and maintaining a system for providing training and legal advice to county prosecutors, by chairing the

Computer & Telecommunication Coordinator program, which consists of county prosecutors assigned to prosecute computer crimes.

(c) The SDAG shall monitor current cases, laws and proposed legislation concerning high technology and computer crimes, and identify further legislative needs and recommend to the Director of the Division of Criminal Justice and the Attorney General legislative proposals to address such needs in this area.

5. Investigations Division. The Investigations Division shall be comprised of three investigative units. These units shall be known as the Incident Response Unit (IRU), the Cyber Crimes Unit (CCU) and the Internet Predatory Crimes Unit (PCU).

6. Incident Response Unit (IRU). The IRU shall be reflected as a unit within the Division of Criminal Justice and shall be led by a DCJ Supervising State Investigator. The IRU shall be comprised of both DCJ State Investigators and DSP detectives. It may also include investigators who are members of the DSP task force, such as FBI agents or members of county or municipal law enforcement agencies. Personnel assigned to the IRU shall:

(a) Conduct and assist in investigations where computers, networks, telecommunication devices, and other technological devices are the instrument or target of the commission of criminal acts against network resources critical to the

function of private or public entities;

(b) Provide training for the New Jersey law enforcement community regarding network intrusion related crimes and their impact on private and public entities;

(c) Provide corporate outreach services to educate and inform the public and private sector, as well as institutions of higher education within the state, as to the dangers and vulnerabilities of wired and wireless networks;

(d) Establish and maintain a state cyber security response group for incident response statewide in the event of significant network intrusion. Nothing in this Directive shall prevent the IRU from collaborating with any future efforts of the Office of Information Technology (OIT) or any other entity in the area of cyber security;

(e) Provide local assistance to out-of-state authorities investigating incidents of network intrusion emanating from, terminating in, or occurring through, the State of New Jersey;

(f) Provide training and assistance to federal, state and local law enforcement agencies in the enforcement of criminal laws relating to computer crimes through forensic collection, recovery, processing, preservation, analysis, storage, maintenance, and presentation of digital evidence;

(g) Conduct computer forensic examinations and the analysis of digital evidence as it pertains to technology related crimes in the State of New

Jersey, by providing forensic examination of digital media pursuant to consent or search orders, or judicial, executive, or administrative seizures;

(h) Monitor current laws and proposed legislation concerning high technology and computer crimes, and identify further legislative needs and make recommendations to the SDAG and DSP Bureau Chief for legislative proposals to address such needs in this area; and

(i) Conduct research and development projects to advance the understanding of the New Jersey law enforcement community about computer crime methods and trends, and enhanced investigation techniques through advanced technology.

The IRU shall confer with and be guided by the Legal Affairs Division in determining the appropriate legal implications and requirements of the use of advanced technology before deploying such measures.

7. Cyber Crime Unit (CCU). The CCU shall be reflected as a unit within the Division of State Police and will be led by a DSP Lieutenant. The CCU shall be comprised of both DCJ State Investigators and DSP detectives. It may also include investigators who are members of the DSP task force, such as FBI agents or members of county or municipal law enforcement agencies. Personnel assigned to the CCU shall:

(a) Conduct and assist in investigations where computers are utilized

for the commission of fraud and identity theft, through the use of the Internet or any computer device;

(b) Provide training for New Jersey law enforcement agencies in investigations where computers are utilized for the commission of fraud and identity theft;

(c) Provide corporate outreach services to educate and inform the public and private sector, as well as institutions of higher education within the state, as to the dangers and vulnerabilities of online fraud and identity theft;

(d) Establish and maintain a mechanism for receiving Internet fraud and identity theft complaint case referrals from any public or private entity as required by the Identity Theft Protection Act, including referrals from outside agencies, such as Internet Crime Complaint Center (commonly referred to as the "IC3"), and the Federal Trade Commission;

(e) Provide local assistance to out-of-state authorities investigating incidents of online fraud and identity theft emanating from, terminating in or occurring through the State of New Jersey;

(f) Conduct computer forensic examinations and the analysis of digital evidence as it pertains to technology-related crimes in the State of New Jersey, by providing forensic examination of digital media pursuant to consent or search orders, or judicial, executive or administrative seizures;

(g) Provide training and assistance to federal, state and local law

enforcement agencies in the enforcement of criminal laws relating to computer crimes through forensic collection, recovery, processing, preservation, analysis, storage, maintenance, and presentation of digital evidence; and

(h) Monitor current laws and proposed legislation concerning high technology and computer crimes, and identify further legislative needs and make recommendations to the SDAG and DSP Bureau Chief for legislative proposals to address such needs in this area.

The CCU shall confer with and be guided by the Legal Affairs Division in determining the appropriate legal implications and requirements of the use of advanced technology before deploying such measures.

8. Internet Predatory Crimes Unit (IPCU). The IPCU shall be reflected as a unit within the Division of State Police and shall be led by a DSP Lieutenant. The IPCU shall be comprised of both DCJ State Investigators and DSP detectives. It may also include investigators who are members of the DSP task force, such as FBI agents or members of county or municipal law enforcement agencies. Personnel assigned to the IPCU shall:

(a) Conduct investigations where computers, telecommunication devices, and other high technology instruments (including the Internet), are the vehicles for the commission of criminal acts perpetrated against children;

(b) Serve as the lead representative for the previously established

Internet Crimes Against Children (ICAC) Task Force, maintain and manage the ICAC grant and oversee compliance of all administrative and operational guidelines as mandated by the Department of Justice, Office of Juvenile Justice Delinquency Prevention;

(c) Provide training for law enforcement agencies throughout the state in investigations where computers are involved in the commission of crimes against children;

(d) Provide corporate outreach services to educate and inform the public and private sector, as well as institutions of higher education within the State, as to the dangers and vulnerabilities of technology-driven crimes against children;

(e) Provide local assistance to out-of-state authorities investigating incidents of online crimes against children emanating from, terminating in or occurring through the State of New Jersey;

(f) Provide training and assistance to federal, state and local law enforcement agencies in the enforcement of criminal laws relating to computer crimes through forensic collection, recovery, processing, preservation, analysis, storage, maintenance and presentation of digital evidence;

(g) Conduct computer forensic examinations and the analysis of digital evidence as it pertains to technology related crimes in the State of New Jersey, by providing forensic examination of digital media pursuant to consent or

search orders, or judicial, executive or administrative seizures; and

(h) Provide presentations to students, school staff, parents and community groups throughout New Jersey in a proactive effort to foster awareness; provide guidance to children, parents, educators, librarians and other individuals concerned about child safety issues on the Internet; and

(i) Monitor current laws and proposed legislation concerning high technology and computer crimes, and identify further legislative needs and make recommendations to the SDAG and DSP Bureau Chief for legislative proposals to address such needs in this area.

The IPCU shall confer with and be guided by the Legal Affairs Division in determining the appropriate legal implications and requirements of the use of advanced technology before deploying such measures.

Nothing in this Directive shall be construed to prohibit the IPCU from collaborating with other agencies in the effort to protect New Jersey's children and others from online predators or to investigate and apprehend criminals who utilize New Jersey technology to engage in illicit conduct.

9. Intelligence Analyst. The Investigation Division shall also designate an Intelligence Analyst, who will implement and coordinate the AGCCTF intelligence-based policing efforts, including:

(a) Responsibility for all computer files, reporting systems and/ or

programs for the processing of intelligence and investigative data;

(b) Conforming to the policies and procedures for the entry, modification, purging, and auditing of the data contained in the intelligence repository;

(c) Serving as a liaison for all external queries of the intelligence system and disseminating information nationwide on behalf of the AGCCTF to other local, county, state, and regulatory agencies; and

(d) Providing reliable, timely and pertinent analysis of intelligence and investigative data and trends as they relate to Task Force investigations.

10. Training Committee. The New Jersey law enforcement community must be trained in the area of investigating computer crimes. This need extends beyond the ability of the AGCCTF to respond to every computer-related crime in New Jersey. As such, there is hereby established a Training Committee within the AGCCTF, responsible for the coordination of training programs related to computer crime investigation and prosecution.

(a) The Training Committee shall report to the AGCCTF supervisors, the SDAG and DSP Bureau Chief. The Training Committee shall coordinate efforts with the NJSP Training Academy, New Jersey Regional Computer Forensic Laboratory, the Federal Bureau of Investigation, the DCJ Training Academy, the Office of the Attorney General's Advocacy Institute and all other relevant training

resources, to identify training topics and to develop training programs for law enforcement investigators and prosecutors.

(b) The Training Committee shall also organize community outreach programs and speaking opportunities for the IRU, CCU, DTIU and legal staff. All staff members of the Task Force will be made available to participate in the training program to share their specialized knowledge with the New Jersey law enforcement community.

(c) The Training Committee shall also maintain continuing education records for IRU, CCU and DTIU staff. The Training Committee shall ascertain training requirements for IRU, CCU and DTIU staff through recommendations by unit members.

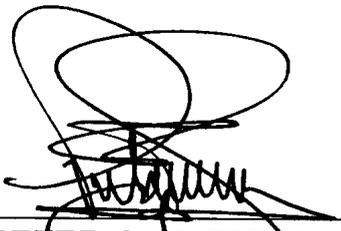
(d) The Training Committee shall be responsible for drafting appropriate grant applications or justification memoranda to ensure timely filings of training applications and requests for travel.

(e) The Training Committee shall make recommendations to the Attorney General concerning training requirements necessary to ensure proficiency and technical expertise of Task Force members.

11. Access to Departmental Resources. The AGCCTF shall be authorized to call upon the expertise and assistance of every division, agency, office, bureau and unit within the Department of Law and Public Safety, and the County

Prosecutors' Offices, in order to carry out its mission. Each division, agency, office, bureau and unit within the Department of Law and Public Safety, and the County Prosecutors and their personnel, are hereby required, to the extent not inconsistent with law, to cooperate with the AGCCTF and to provide such assistance as the AGCCTF may require to accomplish the purposes of this Directive.

12. Annual Reports. In each calendar year, the AGCCTF shall provide to the Attorney General a report as to the activities of the Task Force and its constituent organizational units.



PETER C. HARVEY
ATTORNEY GENERAL

Attest:

13. Stephen Finkel
B. Stephen Finkel
Assistant Attorney General

Date: 12/30/05