National Cybercrime Investigators Program

ABOUT NCIP'S CYBER INVESTIGATIONS PROGRAM

In many ways, the direction of NCIP's Cyber Investigations Program reflects the lessons learned, and the path blazed, by NYPD in its efforts to fulfill its law enforcement charter and organizational mandate to meaningfully respond to constituent complaints of "Cybercrimes".

That is, NYPD launched its NYPD Cyber Investigative Standards Pilot Program, and, in the process, found that the term "Cybercrime" is overbroad and confusing, from an investigative perspective. NYPD also developed the understanding of the "cybercrime" problem that, from an investigative perspective, many "cyber" cases could be investigated and cleared using traditional policing methods and processes, without any meaningful technical "cyber" knowledge, while other cases require deep technical "cyber" knowledge in order to be cleared. Concluding that the term "Cybercrime" should be replaced with less confusing terminology, NYPD coined two new terms for these two types of cases: "Cyber Enabled Crimes" and "Cyber Native Crimes".

Here's what these two terms refer to:

- **Cyber Enabled Crimes** are traditional crimes abetted by cyber tools (e.g., **fraud, scams, larceny, grand larceny, and extortion**); or facilitated by use of cyber tools, like coordination or planning of traditional crimes using digital devices like phones or computers. Cyber Enabled cases, then, can be investigated and cleared using traditional policing methods and processes, without meaningful technical "cyber" knowledge.
- **Cyber Native Crimes**, on the other hand, are crimes (like **cryptocurrency hacking, network intrusion, election tampering** or **data theft**) that could not be committed outside the digital domain. Cyber Native cases require deep technical "cyber" knowledge in order to be cleared.

NCIP's Cyber Enabled Investigations Program, then, is based on the "lessons learned" by NYPD in developing its understanding of Cyber Enabled Crimes, and is executed using the SCIO App and SCIO App Training provided to law enforcement agencies at no charge.

NCIP's Cyber Native Investigations Program, on the other hand, is based on two NCIP initiatives.

- One involves separating the efforts required to conduct a Preliminary Investigation of a Cyber Native case, from the efforts required to fully investigate such a case. The premise here is that a Preliminary Investigation of a Cyber Native case can be accomplished by a Level 1 (or higher) Cyber Investigator, while a full investigation will typically require considerably more technical cyber expertise. This initiative has been accomplished by NCIP's creation of the Incident Data Report Documents, completion of which concludes the Preliminary Investigation Phase of a Cyber Native Investigation.
- The second initiative is to standardize the collection and sharing of information about Cyber Native incidents using the Incident Data Report Documents, because sharing that information will be useful to many other investigations, even if the investigation of the originating case is not completed.

Both of these NCIP programs comply with authoritative guidance in NIST SPECIAL PUBLICATION 800-61, REV 2, "Computer Security Incident Handling Guide", and are based on cybersecurity industry best practices.

info@ncip.tech 504-717-4872
www.NCIP.tech www.e-Ponte.tech