**Mr. Petersen:** The NICE Cybersecurity Workforce Framework, published as NIST Special Publication 800-181, establishes a taxonomy and common lexicon that is used to describe cybersecurity work. The NICE Framework is intended to be applied in the public, private, and academic sectors. In this edition of the NICE eNewsletter, we're profiling Detective Andy Kleinick from the Los Angeles Police Department (LAPD). Andy, thank you for letting us learn more about your career pathway, and how to understand or apply the NICE Framework from the lens of someone who is performing cybersecurity work.

**Detective Kleinick:** Thank you, Rodney.

**Mr. Petersen:** Andy, explain your role and responsibilities as a detective in the Computer Crime section of the LAPD.

**Detective Kleinick:** I am the Senior Detective of LAPD Cybercrime section. I'm responsible for both units within the Cybercrime section. We have two units. One being the investigative unit, which handles what would be considered in California to be 502(c) of the California Penal Code, is basically your unauthorized computer accesses, network intrusions, hacking, theft of data, DDOS attacks, and so on. Our other section is the Digital Forensics section, where we examine all digital evidence, any evidence capable of holding any type of digital information. And I am supervisor over both units.

**Mr. Petersen:** Thank you. And could you say a little more about the size of that actual team in the Computer Crime section, maybe more about the type of roles that those individuals fill.

**Detective Kleinick**: Sure. At the current point, we have 14 people total including myself. It's basically half and half as far as in forensics and investigations. The investigators are pretty much all detectives, anywhere from Detective 1, which is our new detectives through Detective 3, which are the senior detectives, detective supervisors.

We work with a Federal task force, with the United States Secret Service, called the Electronic Crimes Task Force, along with several other state, local and Federal agencies including the FBI, the California Highway Patrol, the LA County Sheriff's Department, and Los Angeles District Attorney investigators to go out and investigate high tech crimes, mostly involving intrusions, hacking, data thefts, major attacks such as malware attacks, business attacks such as email compromises, and so on.

The forensic side are more the geeks. Most of the people who come into forensics have computer backgrounds, and they are the ones analyzing all the digital evidence; be it a tower computer, or the computer inside a motor vehicle. As with other things, the Internet of Things has become so widespread, this constantly changes and upgrades all the time.

**Mr. Petersen:** Describe your career path to becoming a Detective 3 in the Computer Crimes section.

**Detective Kleinick**: With LAPD, everybody starts in the field as a police officer. So, I was in the field for several years, about four years and I was lucky enough to make detective with just four years on the job. Then, once you make detective, you usually go to an area, one of the twenty-one areas in the City of Los Angeles, and you usually move around from table-to-table, from the juvenile table, to robbery, to homicide, to get a flavor of everything you like. From there, I went into auto theft, in the auto theft task force, because I was interested in that. From auto theft, I went into narcotics, and eventually I became a supervisor, which would be a Detective 2, in Internal Affairs.

From Internal Affairs, I went on to become a Commander's Adjutant, which was a way of learning the inner workings of the department. It helps you promote and it helps you learn and meet the people you need to meet. So, that's where I made Detective 3, as a Commander's Adjutant, and from there I went to the Cybercrime Section, because that is something I have always been interested in. I worked in computer technology before I even came on the job, like thirty-five some odd years ago. I worked for a company CMI, which was eventually taken over by IBM, which produced hard drives for the IBM XT and AT, and that's pretty much how it happened. I've been there ever since. Of my thirty-one years on the job, approximately fifteen, approximately half has been in the Cybercrime section.

**Mr. Petersen:** That's terrific. So, how could you envision using the NICE Cybersecurity Workforce Framework to both guide your own career, and maybe in your role as a hiring manager for your organization?

**Detective Kleinick:** Well, the NICE Framework is, first of all, very well written and a nice guide especially for me as a supervisor in cybersecurity. Basically, I happen to be in law enforcement but it's still cybersecurity. Especially for my forensic people, when I hire them I like to know that they have a certain level of skill. Nobody's going to come in here with the level of skill they're going to get once they're here. But, I want them to have at least a base. Besides the fact I teach and use the NICE Framework in my teaching, I also use that as well in my hiring. I'm able to use little bits of that to see if this person is qualified or not.

**Mr. Petersen:** What types of cybersecurity jobs are the most difficult for you to fill in your organization?

**Detective Kleinick**: Definitely the forensic examiners. We have a young department. A lot of people come to me with IT degrees, and some people Masters and above actually. It's not really until recently that IT degrees included any form of digital forensics, and some still don't. So, even the people that come to me with those degrees don't necessarily understand what we do in forensics. So, I have to be able to feel these people out because there's a difference between computer knowledge, cyber knowledge, and even programmers that we've had, and a person that can actually sit at a desk and look at bits of data for ten hours a day trying to piece together the puzzle of a crime. It's two completely different things.

That's kind of why we don't necessarily go out and hire non-sworn personnel for it, because part of the job for a forensic investigator is to put together a crime. A lot of times it's from real small bits of a puzzle. I not only need a good investigator, I need somebody with the ability to understand everything from file structure, to the hardware, and how to deal with the hardware. Sometimes we have to take apart very small pieces of hardware, and obviously put them back together so that they work when we're done with them. I also need someone who is interested in keeping up with the technology. We try to train as much as we can, but the person has to want to go out on their own and be interested in the technology.

**Mr. Petersen:** Are academic degrees, or certifications actually required for your organization, and how do you decide whether or not to require them?

**Detective Kleinick:** We can't require them. That's because of the nature of who we are. We can only require degrees, and they can't be specific degrees. We can only require degrees at a certain level, which I believe, may be captain. Like for me to make senior detective, I had to have so many college units. It didn't matter what it was in, you had to have so many. But, especially in forensics, I do look for people with that kind of background. I've actually had one person, a young officer who came to me, and he was already certified in digital forensics, which I require from my people when they come in. I give them three years to get certified. This person actually came in having done it himself at his own expense. So, I knew right away he was going to be good and he was. He was very good at it coming in. That was the only person in fifteen years who came in knowing the job.

**Mr. Petersen:** How do you and your team keep your skills relevant and up to date?

**Detective Kleinick:** We do a lot of training. We are fortunate our chief is very big on training. When budgets ok it, I send my people to the best training that I can. Working with the US Secret Service, they give us a lot of training as well. The Secret Service runs the National Computer Forensic Institute in Hoover, Alabama. I am also an instructor there. They teach to students from law enforcement throughout the fifty states at no cost to the agency, only the cost of the employee's salary. The Secret Service picks up the check for the hotel, the flight, per diem, and the class. That's a big thing. Some of those classes are quite extensive. There's a beginning forensics class which is actually six weeks long. These are really good, intensive classes.

**Mr. Petersen**: How are you attempting to make your workforce more diverse?

**Detective Kleinick:** I've been blessed in this particular section, we have a very diverse section. It might be because I am looking at someone in terms of an energy, do they really want to do this job, do they really have an interest in cyber; and what they've done in the past. Because of that, we've been lucky, our unit is incredibly diverse, including female investigators. Two of our investigators, our longest-term investigators here are both female, one being female African American. We have every other culture that we can get in this unit. We get cases from Los Angeles, which is a melting pot. It's good to have other points of view in the unit that can assist us with things that a person of a different culture might not understand.

**Mr. Petersen:** What is it you enjoy most about the work you do for the Los Angeles Police Department and as a detective in the Computer Crimes section?

**Detective Kleinick**: I love all things cyber. I'm a geek, and I always have been. I worked in cyber long before I came on the job. I love it because it's not just my work, it's my passion and it's my hobby. I love training new young people in this unit. I'm teaching new officers a whole new way of looking at police work. Really, the future of police work is in cyber. Because there is not one crime out there, from petty theft to multiple homicide that doesn't have some sort of cyber nexus to it. So, we're going to need trained investigators, and I like that idea that I'm part of bringing that out in the twenty-first century police officer.

**Mr. Petersen**: Andy, if you could give advice to a young person who is considering a career in cybersecurity, what would you tell them?

**Detective Kleinick**: Well, if I could make that a little more narrow and say in cybersecurity law enforcement, because I don't think I'm qualified to talk, although I know the private sector, I don't think I'm an expert in public sector, in law enforcement. You have to want to step through the beginning hoops. You have to want to be a police officer first and work your way toward promoting into the investigator part of it, the detective part of it.

If I were in college again right now, I would definitely be looking at, and taking a lot of cybersecurity classes, a lot of ethical hacking classes, I would get my CISSP, I would learn as much as I can about forensics. Some universities are teaching a lot about it, some are teaching none. So, you want to be careful about where you want to apply for school. And then, you want to keep up on everything that's going on because things are changing constantly.

**Mr. Petersen**: Well, thank you so much, Andy Kleinick for sharing some of your perspectives today, your work experience, your careers, and how the NICE Cybersecurity Workforce Framework might apply to a law enforcement organization. Thanks so much today for joining us, Andy.

**Detective Kleinick**: I'm glad I could help you.