TechBeat

February 2019

by JTIC

Table Of Contents

About TechBeat

TechBeat is the monthly newsmagazine of the National Law Enforcement and Corrections Technology Center System. Our goal is to keep you up to date on technologies for the public safety community and research efforts in government and private industry.

Subscriptions:
TechBeat is free. To subscribe, go to www.justnet.org and click on subscribe. If you have questions, call (800) 248-2742, fax (301) 240-6730 or email asknlectc@justnet.org.

Federal Program Manager:
Dr. Mark Greene, (202) 307-3384, mark.greene2@usdoj.gov

Staff:
Managing Editors, Lance Miller and Ron Pierce; Editor, Michele Coppola; Lead Writer, Becky Lewis; Graphic Designers and Multimedia, Amy Salsbury, Pei Miller, Yan Yan and Christian Baker.

The NLECTC System
The Justice Technology Information Center (JTIC), a component of the National Institute of Justice's National Law Enforcement and Corrections Technology Center (NLECTC) System, serves as an information resource for technology and equipment related to law enforcement, corrections and courts and as a primary point of contact for administration of a voluntary equipment standards and testing program for public safety equipment.

JTIC is part of the NLECTC System, which includes the Justice Innovation Center for Small, Rural, Tribal, and Border Criminal Justice Agencies, which focuses on the unique law enforcement challenges faced by those types of agencies; the National Criminal Justice Technology Research, Test and Evaluation Center, which provides technology-related research and testing and operational evaluations of technologies; and the Forensic Technology Center of Excellence, which supports technology research, development, testing and evaluation efforts in forensic science. In addition, a Priority Criminal Justice Needs Initiative exists to assess and prioritize technology needs across the criminal justice community.

The Justice Technology Information Center, a component of the National LawEnforcement and Corrections Technology Center System, is supported by Cooperative Agreement #2014-IJ-CX-K404 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice or Leidos Innovations Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking.

WWW.JUSTNET.ORG

JUSTNET News. Includes article abstracts on law enforcement, corrections and forensics technologies that have appeared in major newspapers, magazines and periodicals and on national and international wire services and websites.

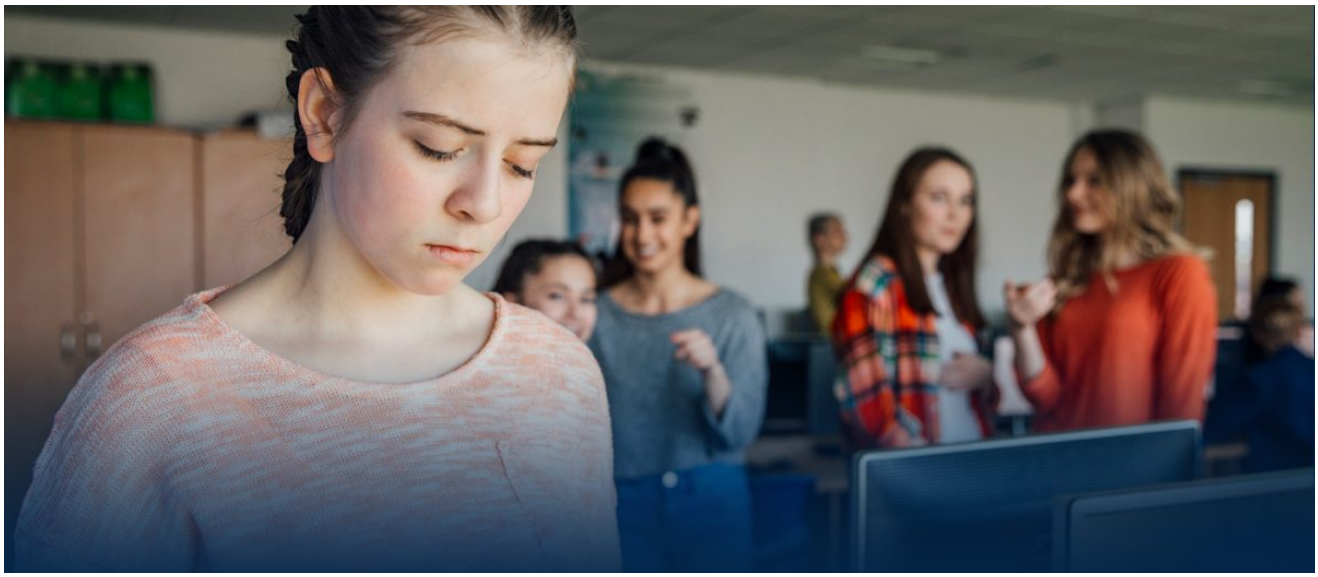
Testing Results. Up-to-date listing of public safety equipment evaluated through NIJ's testing program. Includes ballistic- and stab-resistant armor, patrol vehicles and tires, and more.

Calendar of Events. Lists upcoming meetings, seminars and training.

Social Media. Access our Facebook, Twitter and YouTube feeds for the latest news and updates.

Tech Topics. Browse for information on law enforcement, corrections and courts technologies.

http://www.youtube.com/JUSTNETorg



Cyberbullying and Law Enforcement

Cyberbullying and Law Enforcement

Protecting youths from cyberbullying and exploitation requires a concerted effort by parents, law enforcement, schools and the community. That was a message conveyed by law enforcement presenters during a webinar held in the fall of 2018.

The webinar, Cyberbullying: The Law Enforcement Perspective, was hosted by the Office of Juvenile Justice and Delinquency Prevention, a program of the Office of Justice Programs, U.S. Department of Justice.

Presenters from the OJJDP-funded Internet Crimes Against Children Task Force (ICACTF) program discussed strategies for addressing and preventing cyberbullying. They discussed internet safety, the effects of social media and cyberbullying on a youth's brain, and the impact of sexting and sextortion on youth. ICACTF helps state and local law enforcement agencies develop an effective response to technology

facilitated child exploitation and internet crimes against children.

Supervisory Senior Special Agent Johnny Hall. Hall is with the Virginia State Police and Northern Virginia/Washington, DC ICACTF. He noted that some bullying occurs in the digital world, which presents challenges for law enforcement.

He said most states have laws related to bullying, but can lack policy addressing some of the cyber component. Schools and law enforcement work together to reduce the number of cyberbullying incidents, but they need more resources. School resource officer programs can educate and monitor cyberbullying, but those resources are often strained.

Concerns include:

- Digital devices offer the ability to communicate 24 hours day, making it difficult for children experiencing cyberbullying to find relief.
- Most information communicated electronically is permanent and public because of the way it is stored and kept. If not reported in time it can be difficult to remove.
- Cyberbullying is hard to notice because teachers and parents may not overhear or see cyberbullying taking place.
- Common places where cyberbullying occurs include social media, which offers excellent ways to communicate, but can also be easily abused and used for harassment (e.g., WhatsApp, Instagram, Facebook, Twitter, Skype).

He cited the following community outreach program challenges:

- 39 percent of children or teenagers have given their personal information (e.g., name, sex, age) over the digital world.
- 11 percent have met someone face to face they previously met through the digital world.
- 29 percent say their parents would disapprove if they knew what they did, where they went or with whom they chatted online.
- 36 percent do not discuss online safety with their parents.

(Source: https://www.isafe.org/outreach/media/media_curriculum_effectiveness)

During a question and answer session, Hall agreed that schools and educators should incorporate social media and understanding of the use of social media and digital citizenship as part of an educational curriculum, but noted it may take time to accomplish that.

“It is critical for all of the community to have a participation and understanding of the

interactions with social media. They are a part of everyday life and are not going away anytime soon, and it's better that parents and school systems along with law enforcement take a more proactive role and a more collaborative effort to continue to educate ourselves and at the same time to guide our children," Hall said.

Lt. John Pizzuro. Pizzuro is with the New Jersey State police and is the New Jersey ICAC Task Force commander. He discussed the effects of social media and cyberbullying on a youth's brain, and the importance of providing guidance to young people on use of digital tools. Too much time online can disconnect and isolate youth from traditional social interaction.

"When children are called something on social media and everyone is talking about them with a certain term, it has severe impact on them," Pizzuro said. "When children are being cyberbullied, and being told they are not popular or a nerd, that story becomes their personal story and that is what they believe, and it is difficult for them to get out of that. You have to teach children to reframe and give them the ability to not leave it in that context, because kids can be cruel, and online, that information is there forever. Conversely, if you tell yourself that you are not subject to that in a story, it has a more positive impact."

He said adults need to be more proactive and spend more time educating youth and developing policies. Suggested proactive programs to equip children in navigating the online environment:

- Teach them how to handle cyberbullying and self-care options.
- Focus equal feeling – reframe and don't engage.
- Unplug – focus on other feelings and neurotransmitters.
- Social media and school cellphone policies.
- Be proactive – educators should look for students who are isolated.
- Employ a social media monitor.

Lt. Brian Spears. Spears is with the San Jose Police Department and the Silicon Valley ICAC Task Force. He discussed sexting and sextortion.

Sexting. Sexting typically refers to the sharing of nude or semi-nude and sexually provocative photos or sexually explicit text messages via electronic devices.

Challenges:

- Young people who receive nude/semi-nude sexually suggestive images and sexually suggestive texts and emails are sharing them with other people for whom they were never intended.
- Teens are sending sexually explicit messages and images, even though they know such content often gets shared with those other than the intended recipient.
- Although most teens who send sexually suggestive content are sending it to boyfriends and girlfriends, others say they are sending such materials to those they want to hook up with or even to someone they only know online.

(Source: https://internetsafety101.org/sexting)

Some teens worry about body image. He noted that on YouTube, kids ask the internet audience to tell them if they are pretty or ugly. They rate each other on Instagram.

Digital dating abuse is a form of domestic violence in which youths track others' movements.

"We have junior high and high school students tracking one another's passwords, checking text messages and sending constant messages," Spears said. "The constant control and manipulation, the pressure and coercion is huge, and this has to be recognized now."

Child sex offenders are utilizing technology to further victimize youth. They are capitalizing on the anonymity the internet offers to make direct contact.

Sextortion. Sextortion is the practice of forcing someone to do something, particularly to perform sexual acts, by threatening to publish naked pictures of them or sexual information about them.

Who are the child victims? [National Center for Missing and Exploited Children's CyberTipline sextortion reports, October 2013 through April 2016]

- 78 percent of the reports involved female children and 15 percent involved male children (in 8 percent of the reports, child gender could not be determined).
- Male and female children each ranged in age from 8-17 and had an average age of 15; however, compared to female children, it was less common for male children to be on the younger end of the spectrum.
- In 24 percent of the reports, reporters mentioned that they suspected or knew that additional children were targeted by the same offender.

(Source: https://www.missingkids.org/content/dam/pdfs/ncmec-analysis

/sextortionfactsheet.pdf)

The most common tactic by offenders were the offender threatening to post previously acquired sexual content online (67 percent), and often specifically threatening to post it in a place for family and friends to see (29 percent) if the child did not comply.

Sextortion most commonly occurred via phone/tablet messaging apps, social networking sites and video chats. In a typical incident involving multiple platforms, the offender approached the child on a social networking site where they learn personal information about the child such as who their family and friends are, or where they go to school. The offender then attempted to move the communication to an anonymous messaging app or live stream video chat where they obtained sexually explicit content from the child.

As a result of sextortion, child victims commonly experience negative outcomes, including hopelessness, fear, anxiety and depression. Overall it was indicated in 13 percent of CyberTipline sextortion reports received by the National Center for Missing and Exploited Children, the child victim had experienced some type of negative outcome. Of those reports with some type of negative outcome, it was indicated that about 1 in 3 children (31 percent; 4 percent of all sextortion reports) had engaged in self harm, threatened suicide or attempted suicide as a result of the victimization.

(Source: https://www.missingkids.org/content/dam/pdfs/ncmec-analysis/sextortionfactsheet.pdf)

During a question and answer session, a listener asked how police handle sexting in schools. Lt. Spears said it often depends on which agency is handling it and in which state. He tells his school resource officers to first determine whether the other sexting recipient is an adult or a known juvenile.

“If it is a known juvenile, I encourage the school resource officer to reach out to the parent and bring this information to the forefront at home,” Spears said. “The reason I say that is the parent is the one who furnished the device; usually it is a smartphone. And all too often, parents, I find, constantly want to depend on the school system to provide sex education, and that is a parent’s job. I truly believe it is a parent’s job to talk about sex and the birds and the bees, and the school does facilitate training. We encourage parents and have them respond to the school; that way the phone can be turned over to the parents, and prior to that we erase or factory reset the information. We also tell the parent that the images may be stored on their

cloud system at home, and depending on those images, we notify them that they may be in possession of child pornography if they do not take a proactive approach on erasing this. Usually that really grabs the parents' attention and they respond to the school. We try to keep the parents involved."

Although apps are available to parents to limit what children can see on their phones, presenters said parents need to be vigilant and involved.

"It goes back to, is this child old enough to be given a smartphone? They still make regular phones that you can dial out for safety reasons," Spears said. "I would not just leave it up to an app to monitor and be the virtual parent. It has to be a collaborative effort between the parent and the app and constant communication with the child even on these difficult subjects."

In response to a suggestion that youth/peer leaders (such as older siblings) could educate other children on limiting use of electronic devices, Hall said it could be a good approach to get children to reduce their online activity because youth will listen to their peers.

"Without boundaries, we are not helping the children. We need to work on how that works from within the home, and then include those other resources that are available to us to reinforce that, because the more that children become aware that not only does it start from the home but is also out there in our community and our world around us, they are more accepting to take that approach and eventually those peers will help educate their own, which is really a healthy approach. Community peer groups with other teenagers and kids is a huge benefit because obviously they're going to listen to them."

Resources. Sample resources cited by presenters:

Common Sense, www.commonsense.org

Childnet International, www.childnet.com

ConnectSafely, Connectsafely.org

Cyberbullying Research Center, cyberbullying.org

Family Online Safety Institute, www.fosi.org/

International Association of Chiefs of Police, www.theiacp.org/resources/preparing-and-responding-to-cyberbullying-tips-for-law-enforcement

Internet Crimes Against Children Task Force, www.icactaskforce.org/

ikeepsafe.org

Internet safety 101, internetsafety101.org/

National Center for Missing and Exploited Children, www.missingkids.org

www.netsmartz.org

Safekids.com

StaySafeOnline, staysafeonline.org

stopbullying.gov

Violence Prevention Works!, www.violencepreventionworks.org

Local and federal law enforcement

For additional information, view the webinar here.

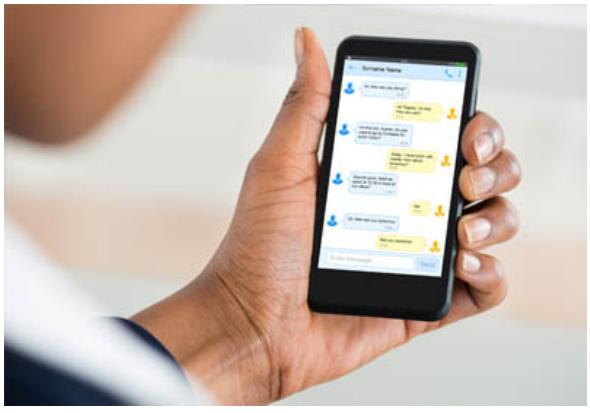
Article photo: iStock.com/KatarzynaBialasiewicz

Main photo: iStock.com/SolStock

FTCoE In-Brief Series Looks at Physical Evidence and Sexual Assault

FTCoE In-Brief Series Looks at Physical Evidence and Sexual Assault

Recent headlines about cold cases solved through family trees and used soda cans have helped push the idea that the only evidence needed to solve any criminal case is a touch of DNA. That's far from reality, and when it comes to sexual assault cases in particular, every piece of physical evidence collected can work together to build a case that will corroborate a victim's account.



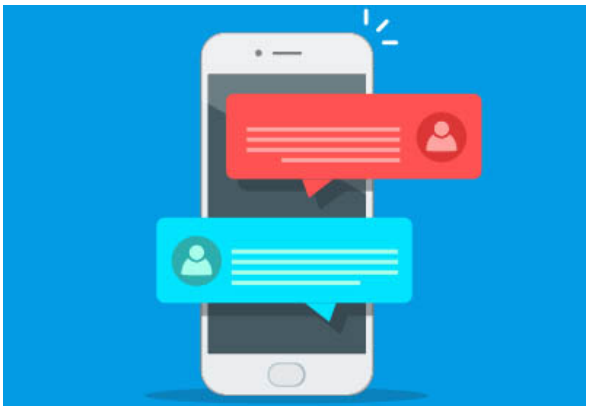
The National Institute of Justice's Forensic Technology Center of Excellence recently released a three-part In-Brief series of reports on the importance of various types of physical evidence in sexual assault investigations. Found on the web here, *Beyond DNA – Sexual Assault Investigations* uses 6- to 8-page reports on physical, biological and toxicological evidence to bring law enforcement, policymakers, legal

professionals and the public an overview of various types of physical evidence and how they may impact sexual assault investigations. In addition, the documents take a look at ongoing NIJ research and provide links to additional resources.

Rebecca Shute, FTCoE innovation analyst, says the idea to create the reports came out of the 2016 NIJ Forensic Science R&D Symposium: "The idea of investigating evidence beyond DNA is always discussed, but never in detail. DNA provides very valuable information, but it's not always present in every case. When a sample is present and CODIS [Combined DNA Index System]-eligible, there's only a hit about half the time. Even if DNA is present and there is a CODIS hit, it may not be probative if sexual contact is not disputed."

In order to ensure accuracy from a legal as well as a forensic standpoint, FTCoE partnered with AEquitas, a nonprofit organization of former prosecutors that provides resources for investigations of gender-based violence and human trafficking. They collaborated on FTCoE's first report in the Beyond DNA series, summarizing the types of physical evidence collected in investigations, and explaining how physical evidence can be used to corroborate victims' accounts. Other reports in the series focused on body fluid identification and toxicology, both of which are used frequently in developing a case, Shute says.

"We wanted the audience of this series to be general," Shute says. "It's more for members of the general public who may be exposed to an investigation at some point in their lives, or for law enforcement officers working sexual assault scenes to encourage them to think about collecting evidence that isn't strictly related to DNA. It's not for forensic toxicologists or lab analysts."



The FTCoE plans to promote the reports to those audiences through a social media campaign, with specific targets for Sexual Assault Awareness Month in April.

"Physical evidence is critical to understanding and communicating the events that transpired during a sexual assault. DNA can provide some but not all of the story; other types of physical evidence can provide unique and valuable information," Shute says. "Biological evidence and toxicological evidence in drug-facilitated sexual assault cases, in particular, can

ultimately lead to just resolutions for these crimes in ways that DNA evidence could not have."

The FTCoE maintains a variety of resources related to sexual assault, which is a key initiative of the Center. Visit here.

Series Highlights

Key points from each of the reports follow.

Part I: The Role of Physical Evidence in Sexual Assault Investigations

Physical evidence may include:

- Physical injuries such as bruising and lacerations. These can, for example, corroborate a victim account of a struggle or determine the location of the incident.
- Digital evidence such as text messages, emails and cellphone records; also data from fitness trackers, cell phone apps and smart home devices. These can establish the whereabouts of the victim and the alleged perpetrator.
- Impression evidence (e.g., fingerprints, shoeprints).
- Trace evidence (e.g., hairs, fibers).
- Other physical evidence (e.g., bedding and clothing).
- Also DNA, blood and body fluids, and toxicology.

Part II: The Role of Biological Evidence in Sexual Assault Investigations

Biological evidence can be found on a victim, on a suspect or at the scene. It typically includes blood from injury or trauma, menstrual blood, saliva, semen, urine and vaginal fluid.

It may:

- Indicate that sexual or physical contact may have occurred.
- Demonstrate that force or restraint may have been used.
- Support or refute victim testimony, such as the type of assault, the physical location and perpetrator characteristics. Note that while it may indicate sexual or physical contact occurred, it does not necessarily indicate a crime and its absence does not indicate no assault took place.

Part III: The Role of Toxicological Evidence in Sexual Assault Investigations

Toxicology testing detects the presence of drugs and toxins through, for example, blood, urine and hair. It can help establish whether a victim was incapacitated or significantly impaired. According to the Bureau of Justice Statistics, an estimated 39 percent of sexual assaults from 2005 to 2010 were what is known as alcohol and drug-facilitated sexual assault (DFSA).

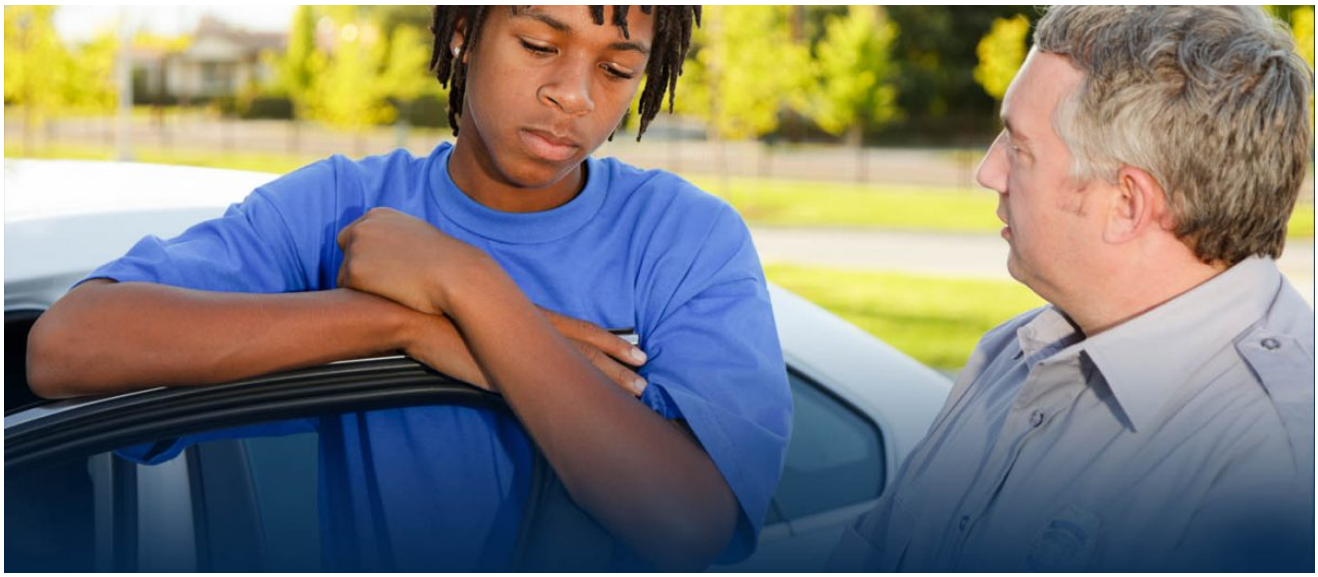
Toxicological evidence can:

- Help establish drug/toxicant concentration thresholds capable of impairing capacity to consent.
- Help investigators understand gaps in victim recall.
- Help corroborate or disprove a scenario. For example, toxicological evidence may be able to estimate a time window for drug exposure.

Note that toxicology reports from blood can provide more detail, but during a shorter timeframe; urine can provide evidence for a longer timeframe, but it is not as precise; and hair can provide an alternative for up to 90 days, but at a further reduction in detail. Also, any prescription or over-the-counter drugs taken by the victim can alter the profile.

Article photo: iStock.com/AndreyPopov, iStock.com/Vladyslav Bobuskyi

Main photo: iStock.com/PeopleImages



Training Helps Lincoln School Resource Officers Learn About Adolescent Mental Health

Training Helps Lincoln School Resource Officers Learn About Adolescent Mental Health

When people hear the term “beta test,” they think of something that’s still in a development stage. But in the Nebraska law enforcement community, BETA has a different meeting: BEhavioral Threat Assessment, a training program that helps law enforcement officers learn better ways to handle individuals experiencing mental health crises. And, Lincoln Public Schools is incorporating a version of this into training for its recently hired middle school SROs.

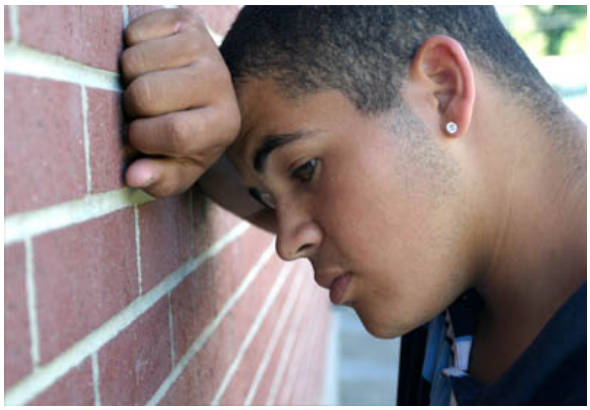
The full BETA program lasts four days, one day covering responding to mental health crises; another on directed violence; a third on a specific timely issue, such as addiction or dealing with the elderly; and the fourth on the options

available for getting help for individuals. The Nebraska Division of Behavioral Health, which provides the training free of charge to law enforcement officers, also offers "mini-BETAs" around the state for officers who can't commit to four days of training away from their agencies.

One of these mini-BETAs brought training specific to adolescent mental health to the six school resource officers hired to work in Lincoln's 12 middle schools. The six SROs were hired as a part of a comprehensive program of community support for schools established through a collaboration between the City of Lincoln and Lincoln Public Schools, including after-school programming and mental health services, in the aftermath of the February 2018 shooting at a high school in Parkland, Fla.

Joseph Wright, Director of Security for Lincoln Public Schools and a former captain with the Lincoln Police Department, emphasizes the importance of not criminalizing behavior for which students need help and assistance. The Lincoln Police Department and Lincoln Public Schools brought the officers on board quickly because of community backing, but still wanted them to receive appropriate training from the National Association of School Resource Officers (NASRO) as well as the more specific local training.

"We want to have a clear differentiation between school discipline and law enforcement action, and ensure the SROs don't get involved in school discipline," Wright says. "And we don't want to criminalize behavior for which students need to receive help. Having mental health issues is not the same as being dangerous."



In order to help the SROs make that distinction, their mini-BETA spent a half-day focusing on adolescent behavior and mental health, and the second half on dealing with individuals who are genuine threats to commit directed violence. Only as an example, Wright likens it to distinguishing between a frustrated autistic child who says he's going to kill the classmates who have upset him, and a student who actually has access to weapons, makes a plan and intends to carry out an attack. He hopes the SRO training has the same positive benefits that the full BETA training has had at the state level.

"We get better outcomes overall because we teach officers not to automatically take people with mental illness into custody, but instead to get them to the resources that they need," Wright says. "One of the things we do during training is bring in individuals who had encounters with law enforcement when they were in crisis, but who are now in recovery. Cops are very experiential learners. We can talk all the theory we want, but when we put someone like this in front of them, they connect.

Wright, who also taught courses at the Nebraska Law Enforcement Training Center on mental health, helped develop BETA training with Division of Behavioral Health staff, before retiring and moving to Lincoln Public Schools 10 years ago. From his position with the state's second largest school district (42,000 students, 60 schools), he worked with Dr. Mario Scalora to create the district threat assessment program. In addition to working with Dr. Scalora, Wright also belongs to and works with the Great Plains Chapter of the Association of Threat Assessment Professionals (ATAP). His presentation for the association's 2019 Winter Conference focuses on how Lincoln has implemented its program, and how the program connects to the Lincoln Police Department and the community. His team focuses on assessing threats, creating safety plans for affected employees, students and parents, and moving everyone involved to a safer place.

"Prevention is hard to measure, but so far, so good. After Parkland, the community reacted very strongly. In addition to our placing the SROs in the middle schools, Lincoln PD added a threat assessment investigator who focuses on school-related cases," Wright says. "On my team, the threat coordinator became a full-time position and we added a high-end social worker to provide planning and support to students that need help and the resources they need who are connected to threat management cases. We've really tried to flesh out the community response. Our whole model won't necessarily work for every school district, but some parts of it might. There are no boilerplate programs that will work everywhere, but schools can still maintain best practices and adapt them to their unique district."

For more information on Lincoln Public Schools' threat assessment program, contact Joseph Wright here.

Article photo: iStock.com/FatCamera, iStock.com/StaffordStudios

Main photo: iStock.com/RichLegg

Victims of Identity Theft, 2016

Bureau of Justice Statistics

This report from the Bureau of Justice Statistics presents data on the prevalence and nature of identity theft against persons age 16 or older in 2016, including how victims discovered the crime; financial losses and other consequences; reporting the incident to credit card companies, credit bureaus and police; the level of distress experienced by victims; lifetime prevalence rates of identity theft; and preventive action taken to reduce the risk of identity theft.

Report highlights include that in 2016, 10 percent of persons age 16 or older had been victims of identity theft during the prior 12 months, and for 85 percent of identity-theft victims, the most recent incident involved the misuse or attempted misuse of only one type of existing account, such as a credit card or bank account.

To access the report, go here.

Main photo: Vicente Barcelo Varona/Shutterstock.com

Latest Issue of NIJ Journal

National Institute of Justice

The *NIJ Journal*, published several times a year, features articles to help criminal justice policymakers and practitioners stay informed about new developments. The *NIJ Journal* presents research-based information that can help inform policy decisions and improve understanding of the criminal justice system.

Each issue will now focus on a single theme, allowing the articles to dive into one specific topic from different scientific points of view. In this issue, scientists and staff share some of the latest developments in policing and law enforcement.

Sample articles include “Body-Worn Cameras: What the Evidence Tells Us,” “Body Armor: Protecting Our Nation’s Officers From Ballistic Threats,” “Improving Officer Safety on the Roadways,” and “Using Officer-Driven Research to Meet Policing Challenges.”

Access articles click here.

Main photo: iStock.com/nojustice