Delivering Innovative Science and Technology Capabilities: Insights from Chris Piehota, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation

By Michael J. Keegan

Technology plays an ever increasing role in daily life. Criminals and terrorists can use this trend to their advantage, posing an even bigger threat to civil liberty and national security. The Federal Bureau of Investigation (FBI) is mobilizing a wide range of advanced scientific techniques and operational technologies to help counter terrorism and criminal threats. Overseeing the FBI's efforts in this area is the Science and Technology Branch (STB).

What is the mission of the STB? What are its key priorities? How does it use science and technology to combat crime and criminal threats? Chris Piehota, Executive Assistant Director of the FBI's Science and Technology Branch, joined me on *The Business of Government Hour* to share his insights on these topics and more. The following is an edited excerpt of our discussion, complemented with additional research.

Would you provide an overview of the history and mission of the FBI's Science and Technology Branch? How does it support the overall mission of the Bureau?

The Science and Technology Branch was established in July 2006 to centralize our various applied scientific and technological capabilities and functions. Shortly after the 9/11 incident, the FBI reviewed its operations regarding how it conducted business post 9/11. We saw a requirement to consolidate its vast science and technology programs under a unified chain of command, a unified leadership model, so that we could better integrate resources.

The STB's mission is very simple: to enable and enhance operations and investigations for our national security programs and our criminal investigative programs. We are an enterprise service provider of technological services and products that enable agents to conduct investigations and operations most effectively.

My main role is to help provide strategic vision and leadership for the branch. We figure out how the branch best fits in with the rest of the FBI's mission sets. The FBI is broken into six primary branches of which the Science and Technology Branch is one of them. Two of the other branches are the National Security Branch and the Criminal, Cyber, Response, and Services Branch. We strive to maintain good strategic alignment with the other FBI primary branches. The STB is comprised of about 6,000 staff members. We're the largest single component that the FBI manages and maintains.

How is STB organized?

The branch has three major components. The Operational Technology Division (OTD) operates as our research and development arm. It also conducts all of our digital forensic work, secure communication, and digital investigative activities. We do fabrication work there. It develops and deploys technology-based solutions to enable and enhance the FBI's intelligence, national security, and law enforcement operations. OTD is staffed with highly skilled and multi-disciplined agents, engineers, electronic technicians, forensic examiners, and analysts. They support our most significant investigations and national security operations with advanced electronic surveillance, digital forensics, technical surveillance, tactical operations, and communications capabilities. While OTD's work doesn't typically make the

"The STB's mission is very simple: to enable and enhance operations and investigations for our national security programs and our criminal investigative programs. We are an enterprise service provider of technological services and products that enable agents to conduct investigations and operations most effectively."

—*Chris Piehota*

news, the fruits of its labor are evident in the busted child pornography ring, the exposed computer hacker, the prevented bombing, the averted terrorist plot, and the prosecuted corrupt official. OTD works extensively with our partners at the local, state, national, and international levels.

The Laboratory Division houses one of the largest and most comprehensive crime labs in the world. It is the CSI of the FBI. We work with our state, local and federal partners to determine standards and practices and protocols for how to collect and maintain evidence. We maintain the Combined DNA Index System (CODIS), which is the nation's DNA database. We do ballistics analysis and shooting reconstructions.

The third component is our Criminal Justice Information Services Division (CJIS). The CJIS Division is our outward facing law enforcement liaison component. The CJIS Division provides a number of services and products to the law enforcement community across the country and for international partners where we manage vast amounts of data and information. For instance, we run what used to be Integrated Automated Fingerprint Identification System (IAFIS), which is now the Next Generation Identification (NGI) system, so we do all of the fingerprint work as well.

We also have a fourth area. We run the Terrorist Explosive Devices Analysis Center in Huntsville, Alabama, a governmentwide service provider to counter improvised explosive device activity around the world.

Any challenges or surprises you would like to highlight?

The challenges are as broad and varied as is the FBI's mission. One challenge is the rapidly evolving pace of technology. What we find is technology is developing and deploying faster and faster. It is challenging our ability to maintain a competitive edge. We also look at integrating mission resources across the FBI enterprise as part of the national security apparatus. These resources serve the U.S. government as well as the FBI as a partner to the law enforcement community, both domestically and internationally. On a day-to-day basis, I ask my people to identify and develop solutions for problems that don't really exist just yet.

What has surprised me somewhat is the complexity and the scope of what the Science and Technology Branch has been asked to do, is doing, and will be asked to do. The challenge to maintain our edge as the counter to national security threats and investigating criminal activities is daunting.

Prior to taking over the STB, you led the FBI Terrorist Screening Center. Would you tell us about your career path? How have you leveraged previous experience into your current leadership role?

I spent six years of active duty in the U.S. Air Force. I trained in a specialized technical field called metrology. This is the study of measurement—of quantifying the world around us and assigning accuracy and uncertainty to various quantities and parameters. When I was in the Air Force, I learned how to be a good leader of people and a good follower of leaders. I left active duty and landed a job at the Kennedy Space Center in support of the space shuttle program, where I spent five years. I was always interested in law enforcement as a career. I applied and was accepted into the FBI in 1995.

After training, I was assigned to the Newark Field Office, working in the counter terrorism and weapons of mass destruction area. I was there through 9/11. In February 2002, I went to FBI Headquarters as a counter terrorism program manager for international terrorism. In 2005, I was assigned to a Washington field office, working in the counterintelligence area. I worked very closely with our intelligence community partners and was promoted to chief security officer for our second largest field office. I then had my initial stint at the Terrorist Screening Center (TSC) before becoming special agent in charge of all FBI operations for Western New York.

After that I became the director of the Terrorist Screening Center, a multiagency organization that was a primary part of the U.S. government's counter terrorism function. I spent a few years at TSC, which was an outstanding assignment for me. I forged partnerships and used technology to identify, detect, and prevent threats around the world. Then one morning I received a very surprising call from the then-FBI Director, who asked me if I would consider serving as the executive assistant director for STB. Because of my experience at TSC—integrating technology with operations—I was able to bring the same customer service and operational support mentality to STB.

What is your leadership philosophy? How do you lead?

My leadership philosophy is based upon two words—mutual support. Everything we do has to help other people be successful and then we hope that they will help us be successful. Everything is about teamwork. Everything is about marshalling people and resources to accomplish our goals and objectives. I know that it happens more gracefully

> "Technology for us is a way to make our investigators and intelligence analysts better at what they do. Technology will not replace them. It augments the Bureau's investigative and intelligence cadres. Technology is not a solution. It's part of the solution."
>
> *—Chris Piehota*

sometimes than others, but what we try to make sure of is that we keep the mission in mind and the mission of the FBI is again to uphold the U.S. Constitution and to protect American society.

I take a three layered approach to leadership. On an interpersonal level, it is critical to be honest. Be objective and be considerate of others. On an organizational level, I ask people to be accountable and results-oriented. I don't think there is anything more unforgiveable than misusing the time of our staff and of our people. They work very hard. Leaders need to make sure that we are getting results for their hard work and efforts. On a professional level, I ask people to be resilient because we have tough jobs. I also ask folks to be enthusiastic because our jobs are very important. People put trust and confidence in us and as such real leaders must lead by example.

Would you outline your vision and key priorities for the Science and Technology Branch?

Our current vision is to be the premier provider of applied science and technology capabilities that address the ever-evolving threat. Our primary drivers, of course, are FBI national priorities. We look at our FBI priorities and then we look at national threat priorities. National threat priorities are evaluated at least annually if not more often. We try to make sure that we are in line with and supporting directly those priorities. We monitor crime trends. We look at emerging crime issues. We try to make sure we provide our partners, customers, and investigative cadre with proper tools and products to identify those threats and counter those threats using science and technology, which complements old-fashion investigative police work.

What is biometrics analysis and how does it assist you in your work? Are there any innovations in this area that you would like to share?

Biometrics is just another way that human beings interact. We have two age-old questions that we ask about each other. First of all, who are you? And are you who you say you are? We've tried to figure this out about each other for centuries—whether it was through secret handshakes, passcodes, different types of identifiers, or authenticators. As the world evolved, our ability to authenticate each other has changed. In the digital age, biographic information is easily counterfeited. Biometrics is a way to remedy this situation. Authentication can be broken down into three areas. It's something you know, something you have, or something you are. What we find is that we try to use combinations of these three areas. Biometrics is something you are and is the way of the future today. It's the modalities of iris scans, fingerprints, and DNA. What we're trying to figure out is how to do this better, faster, more cost effectively. We also have to make sure that we're doing it in line with people's privacy, civil liberties, and constitutional rights.

We also look at other more esoteric things for experimental reasons, such as walking gait analysis. Everyone walks a little bit differently. Voice analysis is another way to authenticate. The shape of the ear can also identify people. It may not be a perfect identifier, but we can use it to triangulate other identifiers to make a good match of an individual.

Would you tell us more about how STB engages in scientific analysis?

As I mentioned, the FBI lab is our premiere law enforcement laboratory. As a leader and standards setter, the lab is a resource developing tools and techniques that the law enforcement community will adopt and use. We also maintain the CODIS Database, which is the National DNA Database. We do a lot of latent fingerprint work where we go in and we extract fingerprints from crime scenes. We extract latent fingerprints from explosive devices. You would be surprised how often we get identification from latent fingerprints off an explosive device. We also do a lot of DNA casework. The FBI lab does forensic response and analysis, and counter terrorism forensic work as well.

The evidence response teams are the FBI's crime scene investigation component. We had multiple teams doing a landfill excavation in the Jacksonville, Florida, area looking for a missing person. Unfortunately, we were unsuccessful, but the team moved hundreds of tons of refuse and did forensic analysis. The lab does crime scene documentation, rescaling, and rebuilding. We do models of crime scenes. One of the more impressive crime scene remodeling projects was the shooting in Aurora, Colorado. It included a scaled down model of the theater, which showed you the trajectory of all rounds fired, the aftermath, the impact.

Integral to your forensic science portfolio is its capacity for operational response. Would you tell us more about the STB's operational response?

I'll give you an example of the Las Vegas shooting. In an event of that magnitude, one if not all three of the STB components will be engaged for direct investigative support, forensic work, field communications, and other types of technology based activities. For instance, our Operational Technology Division can do the digital forensic and information extraction from the device found on the scene. We can collect all of the evidence from the hotel rooms. We can do the ballistic testing on all of the weapons found. We can verify the shooting path. We can do all of the work to reconstruct that event. Also, our Criminal Justice Information Services Division can set up virtual command posts via electronic channels so we can communicate with our state and local partners. We can de-conflict efforts and share information for investigative leads to make sure there aren't any other activities that are maybe planned or haven't been executed. This allows us to be predictive and preventative.

How do advances in science and technology improve the success of law enforcement?

Technology can help us be more accurate, faster, more efficient. We do things differently now than we did just five to ten years ago. Technology can enhance our lives. These benefits can help law enforcement, but unfortunately, technology also allows criminals and national security adversaries to do things that they couldn't do before. It makes them better, it makes them faster, and it makes them better users of resources as well. We try to be a step ahead. We try to be as forward looking and anticipatory as possible. What we try to do is work through partnerships. There is no one organization anymore that has the capabilities, the skills, the resources, or the authorities to combat the complexity of the new criminal investigative environment or the new national security environment. Technology for us is a way to make our investigators and intelligence analysts better at what they do. Technology will not replace them. It augments the Bureau's investigative and intelligence cadres. Technology is not a solution. It's part of the solution.

To learn more about the FBI Science and Technology Branch, go to fbi.gov/about/leadership-and-structure/science-and-technology-branch

To hear *The Business of Government Hour* interview with Chris Piehota, go to businessofgovernment.org.

To download the show as a podcast, go to PodcastOne, iTunes, and businessofgovernment.org.

To view excerpts of the show, go to youtube.com/businessofgovernment.

To read the full transcript of *The Business of Government Hour* interview with Chris Piehota, go to businessofgovernment.org.