Chairwoman Mace, Ranking Member Brown, members of the Sub-Committee, and of the full Committee, thank you for this opportunity to testify before you today.

I am Dr. Doug Gilmer. I am a 35-year veteran of law enforcement with the majority of that time spent with the Department of Homeland Security and Homeland Security Investigations. My career with DHS has focused primarily in two areas; exploitative crime and specifically human trafficking; and national security. I have received a National Intelligence Award from the DNI for Intelligence Integration. I was also recently presented the William Wilberforce Lifetime Achievement Award for my role in helping counter human trafficking globally. I have been most passionate about my work in the field of human trafficking and exploitative crime. In fact, it was this specific mission set that led me to DHS 25 years ago while we operated under our legacy identities. I retired from Homeland Security Investigations in August 2024 where in my last role, I served at the DHS Center for Countering Human Trafficking.

Today I am going to share with you examples of technology case studies that have not been effective, and others that have been. I am also going to share with you some of the obstacles we face integrating technology, technology deficiencies, how and what kinds of technology could be effective in addressing crime, and what needs to be done to improve the technology landscape so it can be scaled for the best the operational outcomes.

To be certain, there is an interconnectedness between illegal immigration, transnational criminal organizations, cross border crime, drug smuggling, human smuggling, human trafficking, etc. Faced with an enormous problem today, and countless numbers of people who were allowed to enter the U.S. during the last administration, many of whom who saw the opportunity they were given to as license to

engage in criminal activity, law enforcement needs help to combat these public safety threats.

Technology can play a key role in combatting cross border crime, transnational criminal organizations, human trafficking, drug trafficking, illegal immigration and illicit finance. Technology can aid in targeting the most extreme threats, identifying trends and patterns, identifying victims, and to analyze vast amounts of data quickly, allowing for a faster and more efficient law enforcement response, while protecting personally identifying information (PII). Technology can also improve employee productivity, mitigate mistakes, improve morale, reduce burnout, and fatigue.

The government has been routinely hampered by its ability to effectively integrate the latest technology, however, and at times has ineffectively used technology in ways that impeded investigative efforts.

When the previous administration took office, a moratorium on immigration arrests was put in place. While this dramatically impacted ICE Enforcement and Removal Operations to do their job, it also impacted Homeland Security Investigations. The authorities we possess under Title 8 are an important law enforcement tool. HSI often uses the authority to further criminal investigations or assist our state and local partners by immediately being able to detain public safety threats from communities while they further their own criminal investigations. This activity stopped in January 2021. We were, for a time, unable to assist our law enforcement partners.

The answer to the situation was to create a computer application by which ICE Officers and HSI Special Agents had to seek permission to make an administrative arrest. The online form had to include the facts of the case and had to provide a detailed need as to why the arrest should take place. The form was then routed through the chain

of command to executive leadership for adjudication based on established protocols. This process took decision making away from the Officer or Agent, who knew the facts of the case, removing their ability to act in specific cases, but also added time and delays in situations which time was often critical. While this was a rapidly developed technological solution, this is an example of an inefficient use of technology to solve a problem that didn't need solving.

There have been technology successes, however. The DHS Center for Countering Human Trafficking (CCHT) recently completed a significant technological upgrade to assist in the issuance of Continued Presence, an immigration benefit provided to foreign nationals in the United States who are believed to be victims of human trafficking. This benefit allows victims of human trafficking to remain in the United States while their case is being investigated, and they provide assistance on their case. I can remember, just a few years ago, Continued Presence was a process that could take well over a year to obtain finalization. The system was dependent on handwritten or typed forms and mailing the application packets from the field, to headquarters, and often back and forth while edits and corrections were being made. Today, through an innovative tech solution, the CCHT has been able to digitize this process and reduce processing time down to as little as three weeks. The team of people at the CCHT and the contractors who developed this system, deserve recognition for their innovation and forward thinking.

Standing in the way of onboarding third party solutions, however, is the current acquisition requirements and the inability to onboard safe and secure technology quickly. This obstacle directly impacts public safety. When technology becomes available to help law enforcement solve critical public safety issues, the time it takes to

acquire the technology, with the way budget cycles work, and the time it takes to receive authorization to actually use the technology after security and privacy vetting, means that by the time it is onboarded, we have missed opportunity and the solution can be outdated. Often, when technology is acquired, it is siloed in a particular agency, component, or division, rather than scaled to provide solutions for the general workforce. Sometimes this is necessary, other times it is due to a lack of financial resources or out of concern for privacy. Even then, there is often no follow-up information sharing from the fruits of the usage of this technology.

Sometimes the issue is a matter of acquisition priority. For instance, in my last field assignment, we only had about five EDDIE machines for HSI personnel statewide. The EDDIE is a portable, fingerprint and photo scanner, about the size of an iPhone, and using cellular technology, allows Special Agents and Officers to check the biometrics of those they encounter and receive very rapid response. This tool can provide the true identity of an individual, a history of law enforcement encounters, help determine alienage and removability, and whether or not the person may have outstanding warrants. Tools like this should be provided to each Special Agent and Officer. Not only can it help in the enforcement of immigration laws, but it saves time, aids in enforcement prioritization, reduces the chance of error, and it also helps law enforcement rapidly identify suspects and mitigate threats to personal safety.

In my personal experience, we often had to rely on non-government organizations and state and local law enforcement agencies, who routinely had better technology than we did, to obtain the information needed to make cases. Not only is this time consuming, but the ability to do so relies solely on personal relationships and it places an additional burden on these organizations to assist us, sometimes in

competition of their own local priorities, while also not being compensated for their efforts and resources.

We are in a new age today with the growth of artificial intelligence. We could benefit from the use of security and privacy compliant AI to enhance identification of critical, time sensitive, law enforcement data. We have a lab at HSI that has implemented advanced technology such as this. The use of this technology is limited to a very small group of users, however. If scaled to an enterprise solution, other DHS law enforcement personnel could utilize this technology to enhance operational outcomes. Rescuing and protecting victims of human-trafficking and other exploitative crimes cannot be achieved without utilizing the most effective and robust solutions available. Using pattern-recognition algorithms that sort through vast oceans of data, this technology could provide invaluable results in real-world and time-sensitive scenarios. The technology could also be used alongside other monitoring systems, such as, body worn cameras, CCTV, drone footage, surveillance footage, social media, and more. This technology could aid law enforcement in tracing and identifying criminal activity and recovering victims while also improving safety of law enforcement personnel by quickly identifying known threats.

Not all illegal immigration looks the way it is portrayed on the news. In fact, immigration fraud, perpetrated to obtain entry into and or lawful status in the U.S., remain in the U.S., or done to otherwise receive some kind of a benefit, remains an issue and the lack of controls is a vulnerability to our immigration system and our national security. This is another area in which advanced technologies, such as AI, could be helpful. Being able to review vast amounts of records and forms quickly, could help identify fraud before the benefit is approved. While not entirely removing the human

factor, the speed at which files could be reviewed and analyzed for fraud, could make a significant difference in identifying and deterring this crime.

If it is concluded that federal law enforcement, already taxed with so many other operational imperatives, cannot handle the production of technology, these solutions could be outsourced to private entities for monitoring, evidence collection, and generating reports to law enforcement. Such efforts currently exist, but they routinely hit up against a number of challenges related to privacy protection and safe harbor. If these efforts are formally vetted and sanctioned, they can be a force multiplier for good.

Transnational crime, cross-border crime, human smuggling, and even human trafficking are financially motivated and interconnected crimes. The same criminal organizations that are trading in drugs and weapons, are also trading in human beings. Not only do we need better tools to identify illicit financial transactions used criminal actors and organizations, but we need better cooperation with the financial industry and FINCEN to improve the flow of information, and the analysis of this information, between the financial sector and law enforcement, but in a way that is safeguarded to protect the privacy of the general public and focused solely on criminal activity. Reinforcing safe harbor provisions is a first step in building greater cooperation between financial institutions, non-governmental organizations, and law enforcement.

One specific area of illicit finance, interconnected to transnational organized crime, immigration, and human trafficking, and can be found in communities both large and small, is the illicit massage industry. Today, we believe there are about 13,000 such illicit businesses throughout the U.S., generating over $5 billion a year in illicit revenue. This industry, largely controlled by the Chinese, is a human trafficking issue, a human smuggling issue, an illegal immigration issue, a human rights issue, a public health

issue, and a national security issue. Many of these illicit businesses are "conveniently" located near military bases, and in the DC, Maryland, and Northern Virginia area, near our most sensitive national security and intelligence installations. As with other forms of transnational crime, the way to attack this issue, is to go after the money. Yet, we lack the resources to do this effectively.

We currently operate systems within DHS, ICE, and HSI, that are deficient in at least four core areas:

1. Siloed systems: We rely on legacy and outdated systems that do not share information, reducing productivity, creating redundancy in workflow, and wasting time.
2. Information accessibility: Difficulty locating information stored in siloed systems prevents law enforcement personnel from gaining valuable insights from current or prior investigations.
3. Lack of standardization: A lack of standardization around workflow processes can create delays in work processes as well as gaps in the completeness of information.
4. Unified resource: Siloed systems prevent personnel from having a single resource from which to find information relevant cases, track productivity, assess investigative outcomes, track evidence, reporting insights, and deadlines.
5. Outsourcing: Current procurement and acquisition programs don't allow for private sector outsourcing in a way that builds capacity to an already taxed system.

DHS, not unlike other agencies, is plagued with a foundational issue, we are sitting on information, and sometimes technology solutions, no one is aware of. In other cases, we know we don't have access to information we need to act. This breakdown in information sharing creates very real issues within the law enforcement environment and can have profound public safety implications. The answer is to adopt systems that not only address the aforementioned, five core deficiencies, but also offers a user friendly and collaborative solution; automated features to define triggers to send approval notices, timelines, and collaboration notices; knowledge access to improve advanced search functions across multiple platforms to identify relevant data; and scalability to improve functionality over time and the ability to integrate new technologies or applications.

If we truly want to be forward leaning with technology to solve crime, then integrating DHS into network of strategically placed automated license plate readers (ALPRs), live video, gunshot detection, drones, and real-time policing software can provide critical investigative leads in cases of human trafficking, drug / illegal weapon smuggling, gang violence, and organized retail theft. These systems capture images of vehicle license plates, along with date, time, and location data, scan them against NCIC or custom hotlists, creating a digital record that can be searched and analyzed. This information can help investigators track the movements of suspects, identify patterns of criminal activity, and connect seemingly disparate incidents. As illustrated in recent news reports, these tools have been instrumental in apprehending violent criminals, gang members, alleged child predators, and even rescuing kidnapped children, demonstrating their potential to make communities safer. There are hundreds of

thousands of sensors across 5,000+ cities in the US that could be leveraged today, with opportunity to deploy more.

Data is critical to law enforcement efforts. Yet, this is an area we often struggle with. We struggle with the ability to collect and analyze data, such as trends, patterns, and prevalence. Without good data analytics, we struggle to identify where resources should be placed to maximize efforts and outcomes. To use a construction analogy, you first have to measure that which you want to fix.

Nowhere is this issue more prevalent than in the area of human trafficking, not human smuggling, not illegal immigration, but human trafficking. Though again, these crimes are often interconnected. Never before in the United States, at least in recent history, has there been more attention to this issue nor have there been more efforts to counter this threat. Yet without systems in place to analyze data, often very siloed data, we fail to identify the methodologies used by traffickers, targeted vulnerabilities of trafficking victims, and even more generally, the scope and prevalence of the problem. The ability to collect and analyze this data would mean law enforcement and their allied partners could better attack the issue with right resources and better serve the victims of this crime.

In some cases, technology and processes are already in place but aren't scaled to meet contemporary requirements. In other cases, we own the technology but are no allowed to use it out of privacy concerns. Facial and pattern recognition technology is one such tool with tremendous potential for solving crimes and recovering victims of exploitative crime. However, the restrictions placed on the use of the technology are so tightly controlled, it is only used in a very small percentage of investigations. Recurrent vetting and targeting is another example. We have built systems in the past with a focus

on national security, but a similar system that conducts vetting on known foreign nationals in the United States who might become public safety threats based on established law enforcement data, such as arrest and conviction data, does not exist.

The best technology, however, is useless, if the technology itself or the evidence and/or data it produces, remains in silos. One of the biggest detriments to law enforcement efforts in combatting crime is the lack of a collaborative data sharing environment and, in its absence, the unwillingness to often share data across law enforcement.

Ranking Member Brown, I applaud your efforts, and the efforts of your colleagues who serve on the Native American Caucus. In that vein, our tribal law enforcement partners face significant challenges. They are vastly under resourced to do the jobs they are sworn to do. Many of our tribal law enforcement agencies are responsible for areas along or near the southwest border and are combating the same crimes other law enforcement agencies do but with far less technology and fewer tools. They can play a vital role in keeping not only their tribal communities safe but also our nation, but need the resources to do it. We need to do more to invest in tribal communities and tribal law enforcement, giving them the tools and training they need, integrating them into collaborative law enforcement efforts, while recognizing their important law enforcement roles and the work they perform. Our First Nation communities and their guardians, deserve better.

All the technology in the world, however, on its own merits, is no good if we don't identify its intended outcomes. The outcomes are what matter. We must determine first the problems we want to solve and what those intended outcomes are. Then we must

acquire and integrate that technology in a collaborative, scalable, and user-friendly format to achieve those goals.

My recommendations are as follows:

1. Break down the silos and encourage collaboration within current and future systems of effort.
2. Ensure the appropriate guardrails are in place around the use of AI and advanced technologies to help guarantee security using a system of checks and balances to help ensure accurate results.
3. Examine the current systems to see what is in place and what can be scaled to achieve results across the enterprise.
4. Utilize academia to help build tools law enforcement needs to do their jobs effectively.
5. Streamline the process by which technology can be acquired and onboard to address the constant and ever-changing threats.

I am proud of my service with ICE and Homeland Security Investigations and of my colleagues there today. My grandfather honorably served a career in this organization, through its legacy identity, and I was honored to carry on that tradition. Then men and women of ICE and HSI are hardworking, dedicated, and have always recognized the importance of relationships with its state and local partners. While lacking technology and an efficient data sharing environment, it has found ways to work closely with other law enforcement agencies across the nation to achieve its law enforcement priorities.

HSI, and ERO, though routinely understaffed and under-resourced for its vast mission, continue to do the work day in and day out while producing outcomes and

statistics far exceeding what should be possible under the constraints they face. I may be bias, but they could be the greatest value proposition in federal law enforcement, and if properly resourced, could do far more good. There is not a more nimble and responsive federal law enforcement agency in the federal government and none that work harder to pursue criminals and criminal organizations, and are more committed to advocating for, and serving the victims of crimes they investigate.