Testimony of

Gregory C. Lisa

Before the
Subcommittee on Digital Assets, Financial Technology and Inclusion

For a Hearing Entitled

"Crypto Crime in Context: Breaking Down Illicit Activity in Digital Assets"

November 15, 2023

Good afternoon, Committee Chairman McHenry, Ranking Member Waters, Subcommittee Chairman Hill, Ranking Member Lynch, and Members of the Subcommittee. Thank you very much for the opportunity to be here today to offer my views on these important issues.

My name is Gregory Lisa, and I am the Chief Legal Officer of DELV, formerly known as Element Finance, a startup company in the decentralized finance space and a research and development studio focused on decentralized infrastructure. I'm a former Partner and now a Senior Counsel at Hogan Lovells, where I specialize in anti-money laundering and sanctions issues, especially in connection with the crypto industry and emerging technology, as well as gaming. My testimony here constitutes my own personal views, and not necessarily those of my employers, clients, or colleagues.

Most of my career has been in government service, starting at the U.S. Department of Justice, initially in the Civil Division and then in the Criminal Division's Organized Crime Section, where I was a federal prosecutor for approximately ten years investigating and prosecuting RICO, fraud, and illicit finance cases. After that, I joined the Consumer Financial Protection Bureau in 2011 as one of its earliest Enforcement Attorneys. I later served in the Financial Crimes Enforcement Network, or FinCEN, initially heading up the enforcement section in charge of money services businesses and casinos – that's where we handled some of FinCEN's first crypto cases. I ultimately became the Interim Director for Compliance and Enforcement within FinCEN.

The Crypto Landscape

We are now some fifteen years after the publication of Satoshi's Bitcoin Whitepaper, and it's been a remarkable decade and a half. Cryptocurrency and other forms of digital assets have had a profound effect on regulatory issues, and they have tested our illicit finance typologies. Along with the proliferation of digital assets and the companies and platforms over the past several years, so have the number of breaches, hacks, fraud schemes, and other bad acts, followed by enforcement actions from a whole host of agencies, civil and criminal, state and federal. Decentralized finance (DeFi) poses a particular set of challenges for regulators and policymakers, given the

absence of any intermediation or custody of funds, certain definitional issues, and open questions as to the proper scope of regulation for DeFi.

There's been much in the press, in politics, and in social media, regarding crypto: some neutral; some of it sanguine; and much of it bad. Candidly, some of the bad press has been accurate. The industry hasn't done itself any favors – ranging from recent criminal prosecutions and convictions; to money laundering and sanctions issues; to breaches and other cyber events; to exploits and rug pulls. We've had several so-called "stablecoins" demonstrate how unstable they can be when they lose their peg; company executives have committed criminal activities with customers' funds and they have taken advantage of the trust placed upon them.

But the news coverage has also overlooked much of the promise of the industry. It has ignored the good actors, and those individuals and companies who are making sincere efforts to understand and follow the law. It's overlooked the fact that many companies and individuals fully appreciate that a healthy industry is one that's sensibly regulated and that meaningfully addresses the real risks in this ecosystem.

The Risk

Depending on whom you ask and the metrics you use, estimates about the amount of illicit finance within crypto vary dramatically. Some have claimed that almost half of all digital asset transactional volume is connected to crime. Others claim that only a fraction of a percent of all crypto transactional volume is illicit.

Both of these extremes are likely wrong. For the lower-end estimates, there are serious caveats and qualifications which are frequently overlooked or misinterpreted. Many of those low-end statistics exclude non-crypto native crime, even if crypto is used for a wider illicit scheme, or if the proceeds of crime start as fiat but then get converted to cryptocurrency. Similarly, much suspicious activity doesn't get counted unless it's conclusively identified by the government in some charging document, such as an indictment or criminal complaint, or if it's in a sanctioned wallet address. And if there's an illicit transaction that goes from wallet A to wallet B, it might then gets considered as licit (or perhaps goes uncounted) if it then moves from wallet B to C, then C to D, and so on. These approaches keep the numerator low.

Many commentators have also raised concerns with the "denominator issue": because many transactions can "hop" from wallet to wallet in a matter of moments, each one of those hops might get counted as a transaction for purposes of overall volume. Wash trading, which provides the appearance of more liquidity, exacerbates this issue. And several transactions get added into "volume" metrics even though they are clearly just crypto investment purchases rather than actual use. All of these make the volume of transactions (the "denominator" of the illicit-to-total volume ratio) artificially high.

Of course, this isn't meant to criticize those companies or commentators who put forward those statistics. Often they spell out their limits and the caveats of their

analyses. But sometimes those qualifiers get ignored in the larger discourse. That's a mistake, because it underestimates the risk, sometimes dramatically. To regulate an industry is to mitigate risks; so it is critically important not to under-appreciate the risk and therefore underreact to it.

By the same token, it is also important not to overreact. Recent statistics cited in major newspapers conflated Hamas-linked accounts with *service providers* to those accounts. That's roughly analogous to saying that if I hold illicit proceeds in a Citibank account, then all of Citibank's accounts should be deemed to facilitate illicit activity. That's a mistake. Some estimates have also taken FinCEN-reported SAR statistics and attempt to extrapolate these as criminal activities, without regard for whether the underlying transaction was actually illegal.

There are fundamental, corrosive problems with overreaction. First, by misapprehending the risk, it misunderstands the challenge that sensible laws can actually address if they are appropriately designed. At bottom, anti-money laundering and countering terror finance is *risk-based*: if you ask any AML professional what a "risk-based approach" means, and they'll tell you volumes. Second, it ignores the real promise that can come from digital assets. The reality is that *every* financial asset and instrument of commerce carries risk.

- Precious metals are fungible, and largely untraceable. To quote FinCEN, "Gold and other precious metals are a highly concealable, transportable, and concentrated form of wealth that can be readily abused by criminals seeking to move and hide dirty money."[1]
- Currency is ubiquitous, and the number one method of choice for drug dealers, human traffickers, money launderers, and most other criminals.
- International trade is the backbone of trade-based money laundering, or TBML, a multi-trillion dollar enterprise.
- Charities serve millions of underprivileged people and important causes, but are also sometimes venues for fraud, money laundering, and terror finance.
- Real estate, owned by Russian oligarchs and drug lords, is a frequent mechanism for laundering illicit proceeds.
- And although shell corporations are a staple of money launderers, fraudsters, and sanctions evaders across the globe, without shell companies, Walt Disney and his brother Roy never would have been able to build a certain theme park just outside of Orlando.

The point here isn't to engage in whataboutism or a similar deflection. Rather, it's to accurately acknowledge that crypto carries illicit finance risk, like, as with gold, shell companies, and charities, can be addressed. The proper role of an anti-money laundering regime is to assess the risk and to build appropriate controls to mitigate it.

[1] FinCEN press release re: In re: B.A.K. Precious Metals enforcement action, December 30, 2015, https://www.fincen.gov/news/news-releases/fincen-assesses-money-penalty-against-precious-metals-dealer-violations-anti-0)

Finally, there is a real chance that overreaction – especially overreaction in regulation – will simply serve to drive crypto underground, offshore, and beneath the radar. Regulation can work, and it should work. But overreaction with regulation can undermine exactly what you're trying to do: it can make compliance impossible; it can divert resources away from real risks; and it can make unregulated environments (and jurisdictions) the only places where companies can survive. As a result, an overreaction can jeopardize national security, and it can make the problem far worse. Ceding ground to China, Russia, or many other jurisdictions might be worse than illicit finance itself.

The 2022 Treasury National Money Laundering Risk Assessment noted that "[w]hile the use of virtual assets for money laundering remains far below that of fiat currency and more traditional methods, … U.S. law enforcement agencies have detected an increase in the use of virtual assets to pay for online drugs or to launder the proceeds of drug trafficking, fraud, and cybercrime, including ransomware attacks …, as well as other criminal activity, including sanctions evasion."

Treasury's 2022 National Terrorist Finance Risk Assessment is similar, noting that "the vast majority" of terror finance is by more traditional means, such as by cash movements, money transmission, and the banking system. At the same time, the report notes that "[w]hile such [crypto] cases are still less prevalent than those involving traditional financial assets, U.S. authorities have identified several instances where terrorist groups and their financial supporters solicited funds in virtual assets, usually through a social media platform or other internet-based crowdsource platform." The report also concluded that "[a]s virtual asset penetration in the overall economy increases, the usage by terrorists is also likely to increase."

And most recently, Treasury's April 2023 Illicit Finance Risk Assessment of Decentralized Finance reiterated that "money laundering, proliferation financing, and terrorist financing most commonly occur using fiat currency or other traditional assets as opposed to virtual assets."

Ultimately, it may be impossible to estimate with any precision how much crypto is used, on chain or off-chain, by criminals and terror financiers. But we do know this: criminals and terrorists are resilient; they're incredibly adaptive; and they're often excellent beta testers for new technology and innovative methods of moving funds. It is not at all surprising that North Korea, Russia, Iran, Venezuela, and others have all made investments in crypto and blockchain technology, and have attempted to use crypto for various forms of illicit activity. Criminals and rogue regimes are incredibly resourceful.

Blockchain Analytics

One thing that is often overlooked is the role of blockchains in not only furthering the underlying utility of cryptoassets and related business models (such as lending, money transfer, and the like), but also how blockchain analytics can be used for the detection and investigation of crime and terror finance. A mantra within every

prosecutor's playbook is to "follow the money": look to see who profits and where the money goes, and that's where the decisions are made and where the most culpable can be found. In organized crime prosecutions, if you want to disrupt the enterprise, you go after the assets, the profiteers, and the organizers. When I was once investigating and prosecuting a violent drug conspiracy, the FBI's wiretap picked up a call between the head of the organization and two mid-level managers who were arguing over profits for a cocaine distribution. The head of the group quickly resolved the dispute: "why are you guys fighting? It's all my money!" That was a pretty useful conversation to play at trial.

Almost all criminal activity (with the exception of crimes of passion and a handful of others) is motivated by profit. And many of the non-greed crimes, such as ideological terrorism, cannot succeed without equipment, logistics, and funding. So "following the money" with thorough financial investigation makes perfect sense if you're trying to detect and disrupt criminal enterprises. That's why anti-money laundering is important.

But the reality is this: traditional financial investigations are difficult and cumbersome – and sometimes ineffective. "Smoking guns" like that drug leader's admission on the wiretap are incredibly rare; those cases are built one brick at a time. Getting bank records and other financial documents often entails guesswork, grand jury subpoenas, and luck. Cross-border traditional financial investigations often depend upon international treaties like Mutual Legal Assistance Treaties (MLATs) or letters rogatory, sometimes with counterpart law enforcement agencies that are insufficiently resourced or who are unwilling to help. All too often those investigations and prosecutions take years, and funds are already transferred into other accounts in other jurisdictions. I once prosecuted a professional international money launderer who openly boasted to me and my case agents that he knew exactly where he could deposit funds without needing a passport; which airports had the most customs agents and surveillance; which jurisdictions would respect international requests for legal assistance, and which would instead leak them to the targets of the investigation. He had memorized extradition patterns, monetary thresholds among different anti-money laundering regulatory regimes, immigration detention standards, and banking practices. And he was able to operate more nimbly than any law enforcement agency.

Blockchain investigations are different. The characteristics and nature of most blockchains provide significant advantages in helping to detect and prevent illicit finance.

- **Transparency/accessibility**: Many blockchain ledgers are completely transparent, and searchable by anyone with access (often anyone with internet access). Law enforcement agents, regulators, the intelligence community, and the public are able to see transactions moving from wallet to wallet, in near-real time. Contrast this with closed, opaque ledgers from traditional financial institutions.

- **Immutability**: Once a block is validated and recorded, it can't be altered, deleted, or otherwise tampered with. Transactional records are permanent, and permanently visible.

- **Reliability**: In part because of its transparency and immutability, blockchain information is highly reliable. Because verification is decentralized, and because of advanced cryptographic techniques, it is extremely resistant to unauthorized access. And unlike an intermediated system where (for instance) a bank holds the only ledger, any potential alteration corruption would be immediately visible.

Even before the proliferation of blockchain analytics companies like TRM, Chainalysis, Elliptic, and others, government agencies were using publicly-available blockchain explorers such as Blockchain.info, Etherscan, Blockcypher, and several others to detect and disrupt criminal activity, to recover victim funds, and to prosecute illicit actors.

And there have been some amazing successes by law enforcement. Justice Department and Treasury Department case files show valuable, effective public/private partnerships where law enforcement and regulatory agencies have used these tools to help prosecute crimes, apprehend criminals, and to intercept and recover victim funds. By way of example:

- Silk Road (dark market case)
- Carl Mark Force / Shaun Bridges (public corruption/extortion/money laundering committed by federal law enforcement agents involved in Silk Road investigation)
- BTC-e/Alexander Vinnik (money laundering DOJ and FinCEN case)
- Welcome to Video (DOJ case involving child pornography website that used Bitcoin for transactions)
- Helix/Coin Ninja (money laundering case in connection with Bitcoin mixing service)
- WannaCry (ransomware)
- Bitfinex (hack of digital asset exchange)

Similarly, many crypto companies, including several that are not currently classified as financial institutions under the Bank Secrecy Act, proactively use those tools on their front ends and in their back-of-house operations to ensure that illicit actors aren't using their platforms. There's a narrative that crypto is full of criminals, and enablers of crime, and that the operators simply don't care whether the systems that they build will be used by illicit actors. I understand that narrative, but I couldn't disagree more: many of the companies in this space care deeply about what they're building, and whom they build it for. Many of us are former law enforcement, and former regulators. Many of us have dealt with victims, and appreciate the harm that financial crime causes.

To be clear, blockchain analytics are not a panacea. Just as there are often no "smoking guns" in financial investigations generally, it's a mistake to think that

blockchain analytics tools are silver bullets. All of those DOJ and Treasury cases have depended on several “non-chain” pieces of information – witnesses, KYC account records from crypto exchanges, communications and social media, search warrants, and extensive other information and tools to make these cases. They offer a critical piece to a puzzle, but not the whole puzzle.

Similarly, there are several things that criminals do and use to frustrate even the most sophisticated blockchain analytics tools, such as chain hopping; privacy coins; mixers and tumblers; and other methods and technologies. Again, criminals are adaptive and resilient. Moreover, being able to trace funds doesn’t mean that you can necessarily identify the wrongdoer or the beneficiaries/profiteers. When people say that illicit funds can be traced to “on ramps” and “off ramps” where people convert crypto into fiat, it doesn’t take into account that many crypto exchanges overseas are non-compliant, or that some illicit actors may not need to go directly to an “off-ramp.”

Current regulatory requirements

As this Subcommittee knows, there is a recurring narrative that crypto is the “Wild West " filled with lawless operators, fraudsters, money launderers, tax evaders, and terror financiers. In some quarters, there have been calls to ban crypto, to regulate it into oblivion, to restrict banks from touching it, and to prevent it from ever getting a foothold into the U.S. financial system. There are concerns with perceived rampant abuse; about victim losses connected with pig butchering and romance scams; regarding ransomware; about environmental concerns; about over-speculation and overhype; regarding criminal activity and use in sanctions evasion and money laundering.

As mentioned previously, the crypto ecosystem and some of its participants have been their own worst enemies. To be legitimate in this space, the industry has to be compliant with existing rules. And perhaps there are new rules that are also required. But it’s simply not true to say that this is the unregulated Wild West, or that there are not rules already in place.

By way of example, many participants in the crypto ecosystem (or those adjacent to it) may be registered brokers and dealers, regulated by the SEC, or futures commission merchants, regulated by the CFTC; or are banks, covered by one or more bank regulators. Many others, such as centralized crypto exchanges, are money transmitters, covered by FinCEN’s rules governing money services businesses. Under the Bank Secrecy Act, all of these entities are “financial institutions” covered by BSA rules which impose several AML/CFT requirements, including the AML program rule, the reporting rules, and recordkeeping requirements.

At a high level, the AML program rule requires covered entities to, at a minimum, (1) maintain risk-based policies, procedures, and internal controls for AML compliance; (2) designate a person for day-to-day AML compliance; (3) provide appropriate training of personnel; and (4) provide for an independent review of the AML program to ensure

that the program is effective and up-to-date. Certain financial institutions, including banks, brokers and dealers, mutual funds, casinos, and others, have other program requirements, such as for customer due diligence or other special program rules.

In addition to maintaining an appropriate AML program, most covered financial institutions are required to file reports with FinCEN, including Currency Transaction Reports (CTRs), and Suspicious Activity Reports (SARs). (The rules have some exceptions for some types of businesses. For instance, precious metals dealers and check cashers are not required to file SARs.) Notably, FinCEN has often praised crypto exchanges for their frequent, detailed, and thorough SAR filings, noting that they have been critical in detecting suspicious activity and in providing important information to law enforcement. Indeed, many successful enforcement actions against crypto companies for illicit finance were significantly furthered by Suspicious Activity Reports.

Third, financial institutions under the BSA regulations are required to make and keep certain transactional records, including regarding funds transfers. Money services businesses are also required to register with FinCEN via the RMSB Form.

Separately, all U.S. companies – regardless of whether they are deemed "financial institutions" under the regulations – are required to comply with OFAC and other sanctions rules. So, for instance, a U.S. company, regardless of its status as a bank or a crypto exchange or a DeFi platform or a shoe store, must follow the OFAC rules. Most of these blockchain analytics tools help to screen for sanctioned wallet exposure, so companies can determine if one of their wallets or if their protocol has interacted with a prohibited wallet address. Many companies also use geo-location and other tools to screen IP addresses from comprehensively sanctioned jurisdictions.

And as noted above, there are several companies in this space–including those that are not regulated as financial institutions under the Bank Secrecy Act–who nevertheless take it upon themselves to screen for illicit activity. They proactively engage with government regulators, law enforcement agencies, and others. They share best practices and they promulgate robust internal controls and frameworks to ensure that bad actors don't get a foothold into their platforms. They do so not because of a specific regulation or court order, but because it's the right thing to do and because they don't want criminals on their systems. Most participants in this space are involved in it for the long term, and they understand that adoption depends on legitimacy and trust.

Simply put, nobody is going to engage with an industry, a service, or a company that looks the other way when it provides liquidity to North Korea's weapons program, or provides a means of funneling money to Hamas or Iran, or is exposed to hacks and rug pulls. Public mass adoption or partnership with larger financial institutions simply will not occur if the crypto industry remains indifferent to fraudsters, human traffickers, terror financiers, money launderers, and sanctions evaders on their networks. If that's the path that crypto chooses, the industry won't survive because the mainstream will never adopt it.

Several overseas jurisdictions suffer from significant noncompliance, whether because of a failure to have adequate rules or a failure (or unwillingness) to enforce them. For instance, Moscow-based Garantex is one of the largest virtual currency exchanges, and is known to be connected to large ransomware actors and darknet markets. The exchange was sanctioned by OFAC in April 2022, and OFAC has sanctioned other noncompliant overseas exchanges, such as Suex and Chatex. Of course, this is not at all unique to the digital asset space: noncompliance with international anti-money laundering standards generally has frustrated global efforts to combat illicit finance in banking, securities, and other financial services industries. But in such a relatively nascent industry, where international standards regarding crypto are still being developed, and where rules, regulatory oversight, and enforcement are so disparate, the effect is much more pronounced: illicit actors engage in regulatory arbitrage, or attempt to stay out of reach of the United States law enforcement despite causing harm to the U.S. public and institutions, and the financial system as a whole.

Cross-border coordination and international leadership

The Financial Action Task Force is an intergovernmental standard-setting organization founded to combat money laundering and terror finance (as well as proliferation finance). Although the FATF presidency rotates every two years, the United States has always held a prominent seat at the table in terms of setting the tone, establishing priorities, and providing leadership. And that leadership is important not just to the FATF, but also to the United States itself. We have an interest in being at the table, and in setting those standards. Combating money laundering, terror finance, and proliferation finance is important globally, and it's critical for the U.S. to be prominent in that dialogue to encourage other countries to live up to international standards.

Some of the standards being promulgated by FATF overbroadly define Virtual Asset Service Providers, or VASPs. For instance, the definition even includes software developers into VASPs, thus subjecting them to impossible rules for obtaining customer information. At bottom, this is where American leadership would be most important, because if unrealistic rules are made, then nobody will follow them and the system as a whole loses value and efficacy.

All of this demonstrates why it is important for the United States to continue to lead in addressing the threat of illicit finance in crypto. An overreaction may be just as bad as an underreaction. Failing to address the actual risks means that the next 9/11 could be attributable to cryptocurrencies. But overreacting and creating inappropriate regulations may mean that the good actors get pushed out, leaving only participants in offshore jurisdictions with substandard or nonexistent AML/CFT controls. If that occurs, we'll never be able to actually address the threats, or place appropriate regulatory regimes around these businesses. At the same time, even if we abdicate this role, we'll nevertheless suffer the effects of illicit finance coming from overseas and affecting the global financial system.

The United States is the center of the international financial system: it is known for its stability, resilience, safety, growth, and fairness. It is home to much of the world's innovation, and its entrepreneurs and businesses. Although it is hardly perfect, the U.S. also leads in anti-money laundering. Other countries and economies look to us for responsible leadership. But there is no guarantee that this will always be so: if we fail in U.S. leadership, either by overreacting or underreacting, then we might relinquish our role to some other country with its own national interests, perhaps hostile to ours. In short, if we as a country don't act responsibly, then we run the risk of losing our place as the global leader in technological development and regulatory oversight. The national security implications of this will be far-reaching, and likely irreversible.

Conclusion

Cryptocurrencies implicate various legal, regulatory, social, and economic issues: securities and commodities classifications, tax rules, possibly environmental impacts, consumer protection, economic stability, privacy, inclusion, and a whole host of other issues. I don't envy the inbox of this Subcommittee in having to consider and navigate all of these concerns. But illicit finance issues are fundamentally different.

And putting aside the legal consequences for a moment, getting this right is existential for the industry as well. People won't invest their money in a system that they don't trust. Nobody wants to provide liquidity to the North Korean government's weapons program or to Hamas, or to have a Russian oligarch or human trafficker or domestic or foreign terrorist financier as their counterparty. Getting this right and addressing this risk is critical to the legitimacy and survival of the industry.

I submit that addressing the issue – rather than ignoring it, downplaying it, or overreacting to it – is critical. Respectfully, let me offer a handful of recommendations:

- First, ensure that the U.S. stays at the forefront of global AML regulation by addressing illicit finance threats with a reasonable, risk-based approach. This means that the U.S. must remain involved in global anti-money laundering enforcement efforts, as well as in ensuring that FATF standards and other international standards are measured and meaningfully address the real risks;

- Second, enable government agencies to enhance their expertise to understand and combat illicit finance, especially in connection with the use of blockchain analytics tools. Provide funding and resources so that criminal law enforcement and regulatory agencies can develop better expertise with enhanced training and better technological resources. Consider whether U.S. government employees should be allowed to possess *de minimis* amounts of cryptocurrency, with appropriate disclosures and other controls, to ensure that they are able to keep abreast of the technology and the applications;

- Third, expand the ability for companies in the crypto space – whether regulated as financial institutions or otherwise – to share information with each other, and to and from law enforcement, under safe harbors if appropriate. FinCEN's 314a program (for law enforcement to the private sector) and 314b program (for private sector to private sector) may provide useful models;

- And finally, let me respectfully submit that Congress consider the issues posed by cryptocurrency – open and transparent ledgers, new business models, pseudonymous actors, and permissionless transactions – not just as a challenge, but as an opportunity. The existing BSA/AML regime, now more than fifty years old, is predicated on intermediating parties, employing know-your-customer rules to gatekeep who should be allowed entry into the financial system and who should be excluded or restricted. The system is incredibly costly: U.S. financial institutions spend about $50B on anti-money laundering compliance programs annually. It is also costly to real people; it is detrimental to social mobility, economic inclusion, and charitable efforts (including remittance flows to needy regions) for hundreds of millions of people across the world. Worse yet, the system is also largely ineffective: recent Basel Institute findings, based on FATF data, provides that the average "effectiveness" score across all assessed jurisdictions stands at just thirty percent. Law enforcement estimates that about two trillion dollars in financial crime is committed each year, but less than one percent of this is caught and stopped.

  The advent of other innovations may further frustrate the efficacy of existing BSA/AML programs and make the current system even more outdated. For instance, generative artificial intelligence deepfakes may make know-your-customer processes less effective in sufficiently verifying customer identity. Conversely, transactional patterns distilled from blockchain analytics may in fact prove more insights regarding actual customer activity, including potentially illicit activity. In short, it may be more meaningful, from a financial crime standpoint, to examine what a customer *does* rather than who the customer *is.*

  Regardless of the success or consumer adoption of cryptocurrencies generally, these technologies may offer the chance and perspective to tear the BSA/AML regime down to its studs and first principles and rebuild a sensible system to address modern technologies and modern illicit finance threats.

Thank you very much for the opportunity to provide this testimony, and I look forward to any questions that the Subcommittee may have.