Talking intelligently

WorldECR in conversation with Crowell partner and former US IG for Intelligence, Michael Atkinson

Before 2024 ended, *WorldECR* was delighted that Michael Atkinson could take time out to explain his previous role as Inspector General of the US Intelligence Community in the Office of the Director of National Intelligence, to discuss similarities between sanctions and export control investigations and those around other national security and white collar crime matters, and to map out the changing national security landscape – all of critical interest to compliance and security professionals as a new year, and a new US administration, begin to take shape.

In President Trump's first term, Atkinson explains, Trump nominated him to be the Inspector General of the Intelligence Community[1] – an appointment that was subsequently approved by the Senate Select Intelligence Committee, and by the US Senate. He started in that position in May of 2018 and held the post until May of 2020.

In that role, Atkinson had jurisdiction over what were then the complete suite of 17, now 18 departments and agencies that comprise the US intelligence community. In such capacity, he says, he 'could look at any programme or any operation or activity across the intelligence community enterprise.'

As a 'typical IG office', says Atkinson, it had (and has) 'divisions for audits, inspections and evaluations, for investigations, and it had its own GC office… And it had a really important role in the intelligence community dealing with whistleblowers.'

But, he says, when Atkinson first took over, the office was in a state of 'public disarray', and was, arguably, failing in its responsibility to whistleblowers in the intelligence community. In response, he says, he took it upon himself to 'sort of "reinvent" the office within the Intelligence Community Inspector General's office, and stood up what was named a Center for Protected Disclosures.'

Because the IG has jurisdiction 'across the intelligence community enterprise', he says, a whistleblower in any of the departments or agencies in the intelligence community could file a complaint with the Office of the Intelligence Community Inspector General.

'Whistleblowing is critically important in the intelligence community… Because so few people have access to programmes or activities [it's important that] the few people who do have that access trust the system to report alleged wrongdoing when they see it. And that they can report it in an authorised way, so that they do not end up leaking it and causing great harm to national security.'

The kinds of issues arising, he said, 'ran the gamut', from grumbles about absenteeism through to more serious complaints around unauthorised disclosures – with the most significant being around then-President Trump's phone call of 25 July 2019 with President Zelenskyy, culminating in a finding by the House Intelligence Committee that the US president had asked his Ukrainian counterpart to 'investigate his political rival, former Vice President Joseph Biden, and a debunked conspiracy theory that Ukraine interfered in the 2016 US election.'[2]

'I took the view,' says Atkinson, 'that any whistleblower complaint about national security… had to be dealt with seriously, because if somebody in the intelligence community is not doing their job, then they are potentially putting national security at risk.'

Michael Atkinson didn't start his career as a public

Crowell & Moring partner Michael Atkinson is the former presidentially appointed and Senate-confirmed Inspector General of the US Intelligence Community in the Office of the Director of National Intelligence. He previously served in senior Department of Justice roles spanning two decades in the National Security Division, the Criminal Division, and the US Attorney's Office for the District of Columbia, where he headed the Fraud and Public Corruption Section. He joined Crowell & Moring in 2021.

'The adversaries or perpetrators tend to be much, much more sophisticated – especially where nation-state actors or foreign intelligence adversaries are involved.'

servant: after graduating from law school, he worked 'on the associate-partner track' at the Chicago-based firm Winston & Strawn but committed to government service after the 9/11 attacks in New York.

First, he joined the criminal division fraud section at the Department of Justice ('DoJ'). This was the 'age of Enron' – a saga which began with the infamous 'memo' to COO Kenneth Lay in 2001, and came to a close with the convictions of Lay and Enron's former CEO Jeffrey Skilling in 2006 for conspiracy and fraud.

During this part of his time at the DoJ, says Atkinson, he was working mostly on 'securities fraud, accounting fraud, FCPA cases – and traveling a lot'.

Some years later, he became an Assistant United States Attorney, and left a decade later as head of the Fraud and Public Corruption Section at the US Attorney's Office in DC. He would go on to become Acting Deputy Assistant Attorney General and senior counsel to the Assistant Attorney General for the National Security Division, dealing with 'overseeing their counterintelligence and export control section, as well as their foreign direct investment folks and their Foreign Agent Registration Act-related issues as well.'

Where does he see sanctions and export controls fitting into that broader national security picture?

From an investigations perspective, says Atkinson, they're very similar: 'You have the same tools available to you in terms of search warrants, subpoenas for domestic entities. And then you have opportunities for proactive cooperation, just as you would in a typical white-collar case, such as a Title III wiretap with cooperating witnesses and undercover agents. What's different is that the regulations are quite technical.'

But there are key differences. One is that in export control and sanctions cases, 'You might see an oil tanker, for example, or oil [or, one might add, an aeroplane] involved, or seized, which you would not in a typical fraud investigation.'

'Another is that the adversaries or the perpetrators tend to be much, much more sophisticated – especially where nation state actors or foreign intelligence adversaries are involved. And it really requires some experience dealing with those.'

As an adviser to companies in the private sector, it goes without saying that the emphasis and approach is different to public service, but the underlying issues and concerns are the same.

'What's important is to build a relationship with law enforcement and federal government before you actually need it.'

'The companies that I work with', he says, 'tend to take broad allegations very seriously because of the legal and reputational harm that they can do. But in the national security space, they take them especially seriously, often because they're government contractors and they understand the consequences to their status as such if they, through their employees, have intentionally violated the law.

'So, the stakes are high [and for that reason] the more sophisticated companies are serious about the support that they give to an investigation, about cooperating with government, and about trying not to cause any further harm to national security when they're making voluntary disclosures.'

This might entail, he says, working proactively with enforcement authorities 'to try to further an investigation that might still be covert on the government side of the house'.

In terms of perpetrators of such threats, they 'tend', says Atkinson, 'to align with the so-called countries of concern: Russia, Iran, North Korea and China'.

'Today, China is the first among equals in that regard. I know the FBI director has talked about how often they open up an investigation into activities related to the Chinese government and related activities.[3] And we see that on the private side as well in terms of cybersecurity attacks, thefts of intellectual property and trade secrets.'

It's certainly the case, says Atkinson, that there are 'opportunists out there who are looking for vulnerabilities at a corporation and sort of a smash and grab'. But, 'When it comes to nation state actors or their agents… we shouldn't underestimate how intentional they are, especially when they are aligned with countries of concern. In my experience, it tends to be strategic. And strategy is not one of just hope and opportunity. It is intentional and it is about identifying valuable targets and working them persistently to try to steal specific information – especially, software.'

As a former IG of the Intelligence Community, Atkinson knows that 'the great challenge for companies that work in the national security space is to understand that it is not a fair fight when they are being targeted by a nation-state actor.'

But, he acknowledges, 'It is a very delicate dialogue, if you will, between the company and law enforcement in terms of understanding when you really do need more resources to deal with a very sophisticated perpetrator, because that [perpetrator] actor will not go away.'

Inside and out

Some companies, says Atkinson, will have their own contacts within government to whom they can reach out, and see 'whether the counterintelligence folks are seeing the same thing from their side'.

What is important, he says, is to 'build a relationship with law enforcement and federal government before you actually need it', especially if you're operating in the kind of company or organisation that's likely to be of value to one of the countries of concern, 'because you never know when you may find yourself the victim of a cybersecurity attack. Or you may find yourself in a situation where one of your employees has done something at the behest of one of these nation state actors and sent something to the wrong place [which puts your company] on the wrong side of export control or sanctions laws.'

That, he says, is the kind of situation that a lawyer with the right kind of experience of government service can help with: 'We would not only identify the solution but also implement it.'

It isn't every company, Atkinson points out, that needs to be cultivating counterintelligence contacts (whether in government or through the intermediary of a consultancy). Universities, also – and not only those undertaking applied but also fundamental research – 'also ought to consider having those contacts, because they are increasingly targeted by nation state actors', as should even the smaller government contractors.

Share and share alike?

But when is the right time to share information with government and how?

'Most of the larger US Attorney's offices have implemented voluntary self-disclosure or whistleblower programmes. The main Department of Justice divisions have their own voluntary self-disclosure programmes, as do the regulatory agencies, such as BIS. The Securities and Exchange Commission has always had a longstanding whistleblower programme… The question, then, is, "To whom should we disclose" suspected violations or concerns?'

In the not-so-distant past, says Atkinson, the answer was 'Main Justice' (aka the Criminal Division of the Department of Justice) or, for companies with publicly traded securities, the SEC.

At the present time, he suggests the situation is more complicated because there are many more choices, which he says 'could potentially become prone to mismanagement or [something analogous to] forum shopping, if you will.'

As things stand, is there

opportunity for companies to disclose to the agencies that companies – or their advisers – predict might give them the easiest ride?

'Well', says Atkinson, 'That wouldn't be my advice, but I could see that going into the calculus. I think you do have to be strategic, of course, but really strategic in such a way that you're mitigating risk, not causing more risk. The calculation ought to be: "Who has the most equities in this issue" as opposed to "Who's likely to give us the easiest time".'

And, of course, companies, banks and others don't typically have insight into the extent to which the agencies share information between themselves – an 'unknown' that can have consequences where, for example, an organisation makes a voluntary disclosure to the US Department of Commerce, 'and the people at the Department of Justice or US Attorney's Office say, "Why didn't you come to us first?"'

That kind of scenario, says Atkinson, '… is a real risk. I've seen it play out. It doesn't necessarily lead to an unfair result, but it can create some uncomfortable conversations if you thought you were doing the right thing in terms of self-reporting, which is a major decision just in itself.'

But Atkinson points out that it isn't in government's interests to make the process of disclosure so intimidating that organisations would fear that, were they to do so, they're bringing 'a whole ton of bricks down on their own heads'.

Most important from government's perspective, he says, is whether, in making its disclosure decision, a company or organisation has acted in good faith, and that it made a principled decision that can be justified: 'If it looks curious, or like there's some hint of gamesmanship, that could lead to a more difficult conversation.'

Contours of service

Michael Atkinson says he was initially attracted to joining Crowell & Moring because of its 'spectacular' government contracts group, which, he says, is 'a great platform in terms of a portfolio of clients in both the defence and technology sectors', as is the firm's privacy and cybersecurity group.

LINKS AND NOTES

[1] The post, which is currently held by an acting Inspector General pending a new presidential nominee, was established under the 2010 Intelligence Authorization Act: www.dni.gov/index.php/who-we-are/organizations/icig/icig-who-we-are

[2] www.govinfo.gov/content/pkg/GOVPUB-Y4_IN8_18-PURL-gpo129303/pdf/GOVPUB-Y4_IN8_18-PURL-gpo129303.pdf

[3] In an opening address to a House Select Committee, 31 January 2024, FBI Director Christopher Wray said, 'The CCP's dangerous actions – China's multi-pronged assault on our national and economic security – make it the defining threat of our generation.'

'It can be beneficial from a national security perspective if your adversaries do not know exactly what you are going to do.'

His own practice, he says, follows the contours of his previous working life in government service, and includes FCPA work, but also 'national security work streams, export controls, sanctions, cybersecurity investigations, and the like.'

Does he expect any change to those contours as the second Trump administration starts to take shape?

The 'countries of concern', he says, will remain 'a concern', adding,

'I think we're still dealing with the aftermath of the specifics of the spy balloon from January, February 2023. It seems amazing that such old school technology [a balloon] got so much public attention… and really focused our society, and our legislature, on the threats from the Chinese government, particularly with regard to advanced technologies, such as artificial intelligence, quantum computing, biotechnology, and the like… I expect that the Trump administration will remain focused on those.'

That will continue to manifest itself, he says, in export control legislation but also controls on foreign direct and outbound investment.

And Russia? 'I think we probably just have to wait and see… The first Trump administration tended to be transactional and unpredictable, and I expect we'll see more of that. Sometimes, it can be beneficial from a national security perspective if your adversaries do not know exactly what you are going to do.'

So long as there's a plan, he adds. 'You just have to hope that there's a plan.'