

On July 20, 2021, General (Ret.) Keith Alexander, Co-CEO of IronNet CyberSecurity, Inc. ("IronNet") was interviewed by Bloomberg Radio 'Balance of Power'. A transcript of the interview is set forth below.

## **David Westin and General Alexander, Bloomberg Radio 'Balance of Power'**

*7/20/2021 1:30pm EST Balance of Power: Protecting Against Cyber Threats (Radio)*

### **David Westin 0:01**

Two days ago, the United States and other Western countries accused actors associated with China of a series of malicious cyber attacks, as they call them, including on Microsoft. Yesterday China responded, calling the accusations quote groundless and quote purely a smear and suppression with political motives. Welcome now a true expert in cybersecurity, he's retired, General Keith Alexander, who served as commander of Cyber Command and then is director of the NSA. He is now the founder of IronNet, a private company that provides protection to companies and governments, for their networks from cyberattacks. General, thank you so much for being back with us, first of all. Give us your take on what's going on in this, right now, war of words but I guess an underlying cyber war of sorts, conflict at least between the United States and China.

### **General Alexander 0:44**

Well first, thank you David. Our country and our allies would not have accused China if we didn't know for sure. So I would tell you, they call them out; they know they did it, Microsoft knows it was China, and we know it was a group that had government affiliations. Of course, China's going to reach back and say, "not us, not us". What concerns me, as you look at this David, is the rhetoric from China is rising. When you look at what Xi Jinping said [into July]. This is growing. It's a growing concern. We've got to fix this cyber area and protect our intellectual property and our money. It's just getting out of proportion. So, this is a national issue. I'm glad the administration is taking it on.

### **David Westin 1:30**

Okay, so we need to fix it. That begs the question and you're the one who knows the answer. How do you fix it because it's a pretty big and complicated problem is it not?

### **General Alexander 1:39**

It's a huge problem, no doubt about it, it's not something that we'll fix overnight. But the key to fixing it is getting the public and private sector to work together. The private sector has got to show the government when they're being attacked and have the ability to do that. In the public sector the government, Defense Department, DHS and the FBI have to see those attacks and block them. That means in real time, think of it as a radar picture and cyber, to help us defend our country and our allies. That's the future of cyber security, we have to get this to network speed. We've got to get before the attack occurs and block them there. It's like shooting down the missile, only doing that in cyber, I think that's the future David.

---

**David Westin 2:24**

So, take us through what your company IronNet does, how do you fit into that chain?

**General Alexander 2:30**

Oh, so one of the things that we do is, if you want to create a radar picture you have to see the unknowns. And that means that things that are getting through, you can block what you know, and everybody is good at that. It's the unknown things that get you. So you need behavioral analytics to see those things that aren't known because there is no signature to go after. Given that you can see those unknowns, you can then anonymize them from companies and share them into the cloud, and by sharing them in the cloud you can see what other companies are getting hit with the same threat. And because it's anonymized you can share that with the government. That creates a radar picture. And that's what IronNet is doing.

**David Westin 3:13**

What is the potential role of our allies in this? I mean, surely they must be having some of these same difficulties?

**General Alexander 3:20**

Yes, and it's growing. You can see, I'm glad that you're not afraid because they're getting hit just as bad as we are, impacted sometimes more from ransomware from China, the theft of intellectual property and from Russia. So when you look at all that, we have to work together. I think perhaps we'll polarize the world in some aspects, but we have to bring like minded countries together, and protect our intellectual property so this is a great way for us to partner with our allies; share that information, extend that radar picture to cover them. Share back and forth. This will be a new world. I think we have to do this, and we have to get going in a very serious manner. So I was really pleased to see that in the executive order on the first page, public private partnership, but I take it a step further. Make it count. Help stop these attacks before they happen.

**David Westin 4:15**

One of things we hear is part of the problem with stopping these attacks is, you know, you have to stop every single one they only have to have one succeed. Is it enough to play defense, do we need to go on offense.

**General Alexander 4:28**

So when I think stop the attack I mean both by defense and on offense.

---

**David Westin 4:32**

Ah.

**General Alexander 4:33**

Right, if they get 100 tries. Ransomware guys can go and they make one work, they hit 15 people they get four to pay, they're on to the next group. We shouldn't give them, we should get one try, stop them, and then work with the FBI law enforcement and with the military, to figure out, what do we do to stop them from doing that again. It's partly in guiding them, but make them pay a cost. Take down their networks if we have to and get like minded countries to work together to help make this happen. That increases the friction, and if you're going to do that, you have to fix the defense. So that's you know that's where I am, you pointed out, David, I led our nation's defense in this area and we didn't have the tools to defend the country. Let's go fix that.

**David Westin 5:25**

I think many people think that we have, perhaps in some ways, the most developed tech sector in the world. We're definitely, Silicon Valley, not limited to that. Is there ways to really leverage that more than we are now, I mean can we get them to help us do this?

**General Alexander 5:42**

Yes, in fact, I'm really pleased to see how the private sector is working together to help do this so I think that's going, of course there's competition and that's good, but the private sector can help make this happen, and you're seeing like minded companies in the cybersecurity thing, start working together. I think that's really important. You hit on a key point. We have the best technology, we're an innovation nation, that's you know Silicon Valley, look what's going on in the Raleigh area, look what's going on in Austin, look what's going on up in Boston. We innovate, China steals that intellectual property to catch up with us. That's what we've got to stop because that's our future. And I think everybody understands that. So first and foremost, we've got to fix that. This is, I think, extremely important for our future.

**David Westin 6:34**

Okay General, it's always such a pleasure to have you with us in no small part because you really teach us. That's retired General Keith Alexander of IronNet.

**Important Information and Where to Find It**

This transcript relates to a proposed transaction between LGL Systems Acquisition Corp. ("LGL") and IronNet. LGL has filed with the Securities and Exchange Commission ("SEC") a registration statement on Form S-4 (the "Registration Statement") that includes a proxy statement to be distributed to LGL's stockholders in connection with LGL's solicitation of proxies for the vote by LGL's stockholders in connection with the proposed business combination and other transactions described in the Registration Statement, as well as a preliminary prospectus relating to the offer of LGL's securities to be issued to IronNet's stockholders in connection with the completion of the proposed business combination described in the Registration Statement. After the Registration Statement is declared effective, LGL will mail the definitive proxy statement/prospectus to stockholders of LGL as of a record

---

date to be established for voting on the proposed business combination. LGL also will file other relevant documents from time to time regarding the proposed transaction with the SEC. INVESTORS AND SECURITY HOLDERS OF LGL ARE URGED TO READ THE PRELIMINARY PROXY STATEMENT/PROSPECTUS AND, ONCE AVAILABLE, THE DEFINITIVE PROXY STATEMENT/PROSPECTUS AND OTHER RELEVANT DOCUMENTS THAT HAVE BEEN OR WILL BE FILED BY LGL FROM TIME TO TIME WITH THE SEC CAREFULLY AND IN THEIR ENTIRETY WHEN THEY BECOME AVAILABLE BECAUSE THEY CONTAIN OR WILL CONTAIN IMPORTANT INFORMATION ABOUT THE PROPOSED TRANSACTION. Investors and security holders will be able to obtain free copies of the proxy statement/prospectus and other documents containing important information about LGL and IronNet once such documents are filed with the SEC, through the website maintained by the SEC at <http://www.sec.gov>. Copies of the documents filed with the SEC by LGL when and if available, can be obtained free of charge on LGL's website at <https://www.dfns.ai> or by directing a written request to LGL Systems Acquisition Corp., 165 Liberty St., Suite 220, Reno, NV 89501 or to [info@dfns.ai](mailto:info@dfns.ai).

#### **Participants in the Solicitation**

LGL and IronNet and their respective directors and executive officers, under SEC rules, may be deemed to be participants in the solicitation of proxies of LGL's stockholders in connection with the proposed transactions. Information regarding the persons who may, under SEC rules, be deemed to be participants in the solicitation of proxies from LGL's stockholders in connection with the proposed transactions described in the Registration Statement and the interests that such persons have in the proposed business combination are set forth in the proxy statement/prospectus included in the Registration Statement.

#### **No Offer or Solicitation**

This communication shall neither constitute an offer to sell or the solicitation of an offer to buy any securities, nor shall there be any sale of securities in any jurisdiction in which the offer, solicitation or sale would be unlawful prior to the registration or qualification under the securities laws of any such jurisdiction.

#### **Forward Looking Statements**

This transcript includes "forward looking statements" within the meaning of the "safe harbor" provisions of the United States Private Securities Litigation Reform Act of 1995, including, without limitation, statements regarding IronNet's business combination with LGL. When used in this transcript, the words "estimates," "projected," "expects," "anticipates," "forecasts," "plans," "intends," "believes," "seeks," "may," "will," "should," "future," "propose" and variations of these words or similar expressions (or the negative versions of such words or expressions) are intended to identify forward-looking statements, including statements relating to IronNet's future financial performance. These forward-looking statements are not guarantees of future performance, conditions or results, and involve a number of known and unknown risks, uncertainties, assumptions and other important factors, many of which are outside LGL's or IronNet's management's control, that could cause actual results or outcomes to differ materially from those discussed in the forward-looking statements. Important factors, among others, that may affect actual results or outcomes include: the inability to complete the transactions

---

contemplated by the proposed business combination; the inability to recognize the anticipated benefits of the proposed business combination, which may be affected by, among other things, the amount of cash available following any redemptions by LGL stockholders; the ability to meet the NYSE's listing standards following the consummation of the transactions contemplated by the proposed business combination; costs related to the proposed business combination; IronNet's ability to execute on its plans to develop and market new products and the timing of these development programs; IronNet's estimates of the size of the markets for its products; the rate and degree of market acceptance of IronNet's products; the success of other competing technologies that may become available; IronNet's ability to identify and integrate acquisitions; the performance of IronNet's products; potential litigation involving LGL or IronNet; and general economic and market conditions impacting demand for IronNet's products. Other factors include the possibility that the proposed transaction does not close, including due to the failure to receive required security holder approvals, or the failure of other closing conditions. The foregoing list of factors is not exhaustive. You should carefully consider the foregoing factors and the other risks and uncertainties described under the heading "Risk Factors" in the Registration Statement, and other documents filed by LGL from time to time with the SEC. These filings identify and address other important risks and uncertainties that could cause actual events and results to differ materially from those contained in the forward-looking statements. Forward-looking statements speak only as of the date they are made. Readers are cautioned not to put undue reliance on forward-looking statements, and neither LGL nor IronNet undertake any obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise, except as required by law.