**Filed by LGL Systems Acquisition Corp.**
**pursuant to Rule 425 under the Securities Act of 1933**
**and deemed filed pursuant to Rule 14a-12**
**under the Securities Exchange Act of 1934**
**Subject Company: LGL Systems Acquisition Corp.**
**Commission File No. 333-256129**

On May 10, 2021, General (Ret.) Keith Alexander, Co-CEO of IronNet CyberSecurity, Inc. ("IronNet") was interviewed by Bloomberg Technology. IronNet intends to make the link to this interview available to investors. A transcript of the interview is set forth below.

**Bloomberg Transcript – General Alexander on Bloomberg Technology, May 10, 2021**

**Emily Chang, Bloomberg Technology**
We've got another special guest here to talk about this, General Keith Alexander, founder and chair at IronNet Securities. General Alexander, of course, served as the Director of the National Security Agency, Commander of U.S. Cyber Command, among other notable roles in protecting our country. General, we were talking to William about what the White House, but more so what the government could do at this moment. Having been in that position, what can they do at this point--what are they doing right now behind the scenes?

**GEN (Ret.) Keith Alexander, Co-CEO of IronNet Cybersecurity**
So, I think the biggest thing that they can do, and what we need to do as a nation, is we need to figure out how to work together between the public and the private sector. The government's job, specifically the Defense Department and Cyber Command, is to defend the country from attacks, but they can't see those attacks and [times] to do something about it. As a consequence, it's incident response. That's too late. So, we need to build, in my words, a radar picture--an air traffic control picture—of a catch coming into our country from the private sector side in an anonymized way that can be shared with the government so they can respond. This is really important because I think our nation is going to be continuously tested in this space, as you mentioned, [solar when] you look at the Microsoft hack, you see a number of different attacks by China and by Russia, and by groups like the DarkSide, that are hitting us with ransomware. Yet right now, every company is defending itself. That's crazy. We have to work together, like a radar picture, show the government what's coming after us, and allow the government the opportunity to defend this country.

**Emily Chang, Bloomberg Technology**
When you look at this hack, what do you see here? What is at stake, and does this look different than other ransomware attacks to you?

**GEN (Ret.) Keith Alexander, Co-CEO of IronNet Cybersecurity**
Well it's interesting listening what Mike said, I kind of agree with him on parts of it. I think they went after this, seeing it as a target, they got in, probably through phishing, they got in, they spread throughout that, they grabbed information, they brought it back, and they thought "ooh this is a lucrative target." I think they underestimated how big a target this would be for our nation. And as a consequence they probably put themselves into an area where they now will be aggressively pursued by the FBI and others. So that, I think was overseen. The issue you brought up with them though, Russian involvement--almost for sure some of these folks came out of Russian hacker groups, the GRU, SVR or something like that. They're Moonlighting, or they're already out, but if they're in Russia working this, the government, almost for sure knows what they're doing. So, this is something we have to get out in front of, we have to attribute, and hold these people accountable. We need to make them pay a price, if we're ever going to get this to stop. The only way to do that is to catch them in time to stop them.

---

**Emily Chang, Bloomberg Technology**
Do you have any indication here that there was any other motivation other than profit? For example, in the worst case, did they intend to blow up the pipeline, or are they just trying to make a buck?

**GEN (Ret.) Keith Alexander, Co-CEO of IronNet Cybersecurity**
Well, I would say most probably just trying to make money off of two areas: encrypt the data and make them pay for that, steal data and make them pay to get it back. So those two, you know, they're going to get paid twice for this thing, or they're going to try to. It could be if you step back, the question that you asked us one that [really] deserves merit, something that has to be looked at. Is this being used as a test to see--can they get in? FireEye cleans it up. Can they maintain access even after the cleanup, and can they do something going from the IT system, which is what they did, over into the OT system? So I think this is a good place where the White House has actually done a good job in bringing this together, as one of their 100 day things: let's go after the energy sector, bring IT, OT together and go after this, create that collective defense for the energy in the oil and gas industries. So, I think that's the right approach that the White House has, but we have to go beyond that, in my opinion.

**Emily Chang, Bloomberg Technology**
It does make you think about the worst case scenario, when a company that's using computers connected to the internet does something as important as transports fuel. What is the worst case scenario, in your view?

**GEN (Ret.) Keith Alexander, Co-CEO of IronNet Cybersecurity**
Well, I mean shutting down the network that they have is, you know, about as bad. Could they do things to the industrial control systems? The concern the government has, and why they're putting a focus on it, absolutely want to do that. I'll tell you my experience. The energy sector at large, and I deal with a number of them, they are laser focused on defending the grid in other parts of our sector. I am singularly impressed with the CEOs of many of these companies leaning forward and saying, "we'll work together to defend this nation, we'll share that with the government." So they've got the right approach. We got to help them cross that bridge from the private sector, the public sector to actually do that. Bad things can happen, for sure. You see that in hospitals, industrial control systems--it could be the same in the energy, oil and gas knowledge. But I am impressed with the way the energy sector and the oil, and gas are working, but they can't do it by themselves, and that's today what's happening. Every company out there is defending itself, and it can't get that information to the government in time for the government to help stop it. We've got to change that way, the way we're doing business, it's got to change. Real time collective defense, I think, is the future for cyber security.



---

**Emily Chang, Bloomberg Technology**
So, let's talk about then, the Colonial Pipeline itself. They're saying they should be able to get back online, by the end of the week. We don't know yet if they've paid this ransom. What approach should they take? Should they pay, do you know if they've paid, and how long after that, does it normally take for a ransomware victim to get back online?

**GEN (Ret.) Keith Alexander, Co-CEO of IronNet Cybersecurity**
So, what they're going through, is they have to go through all the systems that were infected, rebuild those systems, clean them out, clean all the malware out. FireEye,

Mandiant portion of FireEye, I'm sure Kevin Mandy and his teams are all over this, they're great at that. End up doing this together. That's one step. I think they won't pay, but I don't know that for sure. I think that they're cleaning it, and they will do that. But then the second question is, what about that 100 gigabytes of data? What do they do about that? That was stolen, it could be given out. And I think again, I don't know if they're going to pay or not, I think they'd be reluctant to pay. I think that's where government's got to step in and help Colonial, they're a victim here, and we can't treat them like they're the bad guys--they're the victim. A nation state, or people with nation statelike tools, attacked them. And we can't treat them as the bad guy here, Colonial was attacked. And we should hold the bad guys that actually did this accountable, so we have to change that rhetoric is going on there. Colonial is a victim.

**Emily Chang, Bloomberg Technology**
General Alexander, thanks for joining us today.

**GEN (Ret.) Keith Alexander, Co-CEO of IronNet Cybersecurity**
Thank you Emily.

**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@dfnsi.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.