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 30, 2021, General (Ret.) Keith Alexander, Co-CEO of IronNet CyberSecurity, Inc. ("IronNet") was interviewed by ABC News. IronNet intends to make the link to this interview available to investors. A transcript of the interview is set forth below.

ABC News Transcript – General Alexander on "This Week," May 30, 2021

Martha Raddatz, ABC News
So let's bring in the experts on this: General Keith Alexander, former director of the National Security Agency, and the first commander to lead US Cyber Command, Niloofar Razi Howe, Cyber Security Fellow at the New American Think Tank, and ABC contributor Tom Bossert, who served as homeland security adviser to President Trump. Welcome to all of you. General Alexander, I want to start with you, and I want to start with those cyber-attacks. Americans realize how serious these cyber-attacks can be with the Colonial Pipeline, of course, that was a ransomware attack, and they wanted money, but the Solar Winds and now the USAID attacks are different, but so, so serious. What are the hackers after?

GEN (Ret.) Keith Alexander, Co-CEO of IronNet Cybersecurity
I think the Russian hackers are clearly after gaining intelligence on our country, on what the administration is doing, what President Biden is thinking, and what's coming up against Russia, as they prepare, I think, for the upcoming talks between President Biden and Putin. They're stealing information, and you know, it's interesting Martha. This is more blatant than I've seen in my career, they're going after this in the Solar Winds, they think, 18,000 companies and now, as you said 7000 more with this last USAID, attack, and the Colonial Pipeline. Even though they claim that was from hackers, I believe they're associated somehow. They're sending a message, and they're doing it blatantly. They're going after our intelligence system and they're saying, "We can do this." We've got to fix it.

Martha Raddatz, ABC News
And it obviously did expose our vulnerability. So how do you fix it?

GEN (Ret.) Keith Alexander, Co-CEO of IronNet Cybersecurity
I think that's, I like what President Biden put in the executive order, it's a public private partnership. We have to build this solution together. The government can't do it by itself, you see, most of the attacks are going against the commercial sector. The government can't see them. We need to create a radar picture, between the public and private sector that shows attacks in time to prevent them, not talk about them after the breach but prevent the attacks. So, we need to work this together as a team. This is part of our future and we've got to get good at it, and we've got to do it quickly. Both Russia and China are challenging us in this space. And it's shown that we're not ready. I think the executive order hit some part of it. We have to go faster. I, my experience--the private sector is ready. They're pushing forward. So this is where Congress and the administration, the government, and the private sector can really help fix this problem. We need to do it.

Martha Raddatz, ABC News
And Niloofar, I want to ask you I know you've worked with several government agencies and you testified before Congress about the solar winds attack, and said there is simply no unified governmental organization looking at future vulnerabilities. You heard what General Alexander said, what do you think has to happen?

Niloofar Razi Howe, Cyber Security Fellow at the New American Think Tank
Well, Martha for anyone who is still asleep at the wheel, these attacks are a wakeup call, and they're a wakeup call about the new normal that we live in, which is strategic competition in cyberspace is happening every single day, whether it's the theft of defense secrets, intellectual property, personal identifiable information, for example against political dissidents and activists, and it's only going to escalate over time. And the approach we've had, which is this Whack a Mole approach of dealing with issues as they arise, simply doesn't scale to the scope of the problem. We have adversaries who are creative, they're agile, they're bold, they're evading our best defenses, they're using our laws and regulations against us to launch these attacks. So we need to take a different perspective: we need to have, as the General said, a public private partnership, an organization that's looking over the ridge line to identify the future of global threats, the future risk environment, and the vulnerabilities that we face, so that we can develop the defenses for those. And we have great examples, if you look to World War Two, in Tuxedo Park where Alfred Loomis pulled together the best and the brightest to solve the hardest technical problems and arguably changed the course of the war. It has to be public, private, it has to be the best and the brightest, and it has to be strategic not tactical.

Martha Raddatz, ABC News
Tom one of the problems is that public, private. You're protecting government vulnerabilities, and these companies, Colonial Pipeline, don't some companies just look and say, "you don't have a lot of money to protect my system or to upgrade my system. You know, what's $5 million. If I have to pay a ransom."

Tom Bossert, ABC Contributor
Even worse, some companies then view it as a cost of doing business when they do get hit, they pay the ransom and they come back online. So, there's a number of things I'd like to change about the way we look at it, including in that question, are we just protecting individual companies, critical infrastructure, or as I see it, is the United States in a position to do something to stop the adversary? So, if you get closer to the source, you end up with Russia, China, North Korea, Iran behind many of these cyber attacks. As you get farther on the endpoints you get 3 trillion endpoints that we have to protect every day. So, it's a very difficult challenge if everyone's in this alone though, individually against the Russian, Chinese and increasingly combined Russian and Chinese effort, we're going to fail every time. Whether it's an individual government agency or a pipeline operator, there's got to be a collective defense that's generally General Alexander's point of view. So, I agree but public private partnership, suggests that we're going to partner to protect those endpoints. I think we have to do something far more direct, and I would add to the General's answer, I think Russia is doing more than just collecting intelligence. At this point there's evidence that they are carrying out their strategic intent to reduce the US and its influence in power. They're trying to do things to destabilize us and destabilizing big companies like Microsoft is just one way.

Martha Raddatz, ABC News
And I want to move on to that so-called Havana Syndrome. General Alexandra let me, let me ask you quickly about that. The New Yorker had an excellent investigation this week that mentioned those directed energy devices saying "the working hypothesis is that agents of the GRU the Russian military intelligence service have been aiming microwave radiation devices at US officials to collect intelligence from their computers and cell phones, and that these devices can cause serious harm to the people they target." Does that make sense to you?

GEN (Ret.) Keith Alexander, Co-CEO of IronNet Cybersecurity
Yeah it does, and you've seen that, what's called the Havana Syndrome. We've seen that, we've proven that. And they've done it before, and not just against our country but in the same thing, you're talking about Canada and others.

Martha Raddatz, ABC News
It's an incredibly bold move. What do we do about that? How do you punish them?

GEN (Ret.) Keith Alexander, Co-CEO of IronNet Cybersecurity
Yeah. Yeah, so it's the same thing in cyber when you think about it. How do you push back? You've got to give the President and the administration the tools, and they have those, to look at this from a diplomatic, economic, military across the whole spectrum. Covert and overt. What are they going to do? And I think the President has said in a number of meetings, I've been with him on some of those was when he was Vice President, they do it right, they'll get the National Security Council together and say, "Okay what message are we going to send back, and how do we do this in the best interest of this nation?" So, I think that will be done right, but it does need to be pushed back, Martha. You've hit on a key point. This is egregious, this is blatant. And as Tom said, they're telling us, "Look, we don't care. We're going to keep doing this. We will deny it publicly, and we're going to keep doing it."

Martha Raddatz, ABC News
Thank you, General. I want to end very quickly here from the two of you, Tom, what does he do at this summit?

Tom Bossert, ABC Contributor
My advice? He's got to take a position on Nord Stream 2, he's got to prevent Russia from breaking up the European Union, and he's got to do it from a position of strength, meaning he lays out a path in which we apply meaningful sanctions to their oil revenues rushes, and to their sovereign wealth.

Niloofar Razi Howe, Cyber Security Fellow at the New American Think Tank
Look, messages don't work with Putin. Actions do. We have to take action. We have really a good example of how action works in protecting the 2018 midterm elections and shutting down Russian influence operations, taking a whole-of-government approach with the FBI authorities working with the private sector, with DHS and its mandate to protect elections, with Cyber Command and his ability to operate overseas. So, we need to take action. It's not just about delivering this message, and there are three things we can do today, including, by the way, regulate cryptocurrency becomes so important if we want to stop ransomware, which is a scourge right now in cyberspace.

Martha Raddatz, ABC News
Thanks to all of you. It's a really fascinating discussion.

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.