- We're particularly focused on a few issues with the Russians.
    - First is the Russian's history of using poorly controlled, damaging attacks that can potentially spread beyond intended targets. This is what happened in the 2017 NotPetya malware attack, when the Russians infected Ukrainian accounting software with malware that presented as ransomware, but whose purpose and impact was destructive, with no capability to pay a ransom or recover. Russia targeted that malware at Ukraine but it went global, causing billions in damages around the world. That's why we investigate what the Russians do here in the US, and also abroad.
    - Another is the difficulty of determining intent from the kind of intrusion we see. The same access that enables data exfiltration will also usually allow data destruction and other means of shutting a company down. That's why we have a very low threshold for action.
    - Russian cyber actors also are known to gain unauthorized access to sensitive or secret information from victims, stealing that information to then publicly release through proxies with no direct ties to the Russian Government. These leaks are designed to sow discord and confusion among the targeted audiences, while straining ties between allies. Russian malign influence actors use social media, co-opting witting and unwitting surrogates to disseminate their false narratives to exclude or isolate groups. These malign influence operations are part of a broad influence ecosystem that includes Russian diplomats and state media, laundering these false narratives further through seemingly official channels. We continue to identify malign foreign influence actors, expose them and their schemes to social media providers and the public, and use all of our authorities to hold them accountable.
    - Finally, we remain concerned that Russian cyber criminals will target US critical infrastructure - in particular the financial services sector - with ransomware attacks either in support of the Russian government or to take advantage of an even more permissive operating environment in Russia. That's why we're focused on the whole gamut of the threat emanating from Russian intelligence services and cybercriminal groups, and it's also why you should consider the potential for some cyber criminals to potentially act in support of the Russian government when determining your response.
    - Just last Friday, Conti—a well-known ransomware gang—posted the following: "The Conti Team is officially announcing a full support of Russian government. If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use all possible resources to strike back at the critical infrastructures of an enemy."
- Both Russian state-sponsored and cybercriminal actors have used common but effective tactics—including spearphishing, brute force, and exploiting known vulnerabilities against accounts and networks with weak security—to gain initial access to networks. Regardless of which malicious actor is conducting the activity, or the reason you are being targeted, if you take the steps to reduce your risk by implementing cybersecurity best practices and

practicing good cyber hygiene, such as using strong passwords, patching, and updating your software, you can better protect yourself from most malicious cyber activities.

- Let me leave you with a few key takeaways before we move to questions.
- First, we strongly encourage you to review several recent Cybersecurity Advisories (CSA) we've published. We'll send each product to you after this call. These CSAs identify specific Russian malware signatures, indicators of compromise, and TTPs. There is extremely important and tactical information contained in these CSAs that should be read by those responsible for your network's resiliency and defense.
- Second, know your network and what, if any, connectivity, you have in Russia and surrounding territories. Conduct an internal risk analysis to determine how these remote systems and access points should be monitored over the upcoming weeks and months.
- Third, exercise your cyber incident response plan. Please ensure it includes contact information for your primary FBI Albany POC and AlbanyCyber@fbi.gov. It's extremely important for all of us to keep our lines of communication open over the upcoming weeks. If you don't have an incident response plan, we'd strongly encourage you to build one and exercise it. Part of your incident response plan should include knowing if (and who) you will hire as an incident response firm and if (and who) you will hire as outside legal counsel. Working with your legal counsel before an incident is extremely important as it will allow you to define how expeditiously you want to share with FBI.
- Fourth, if you see any social media posts on any platforms that are indicative of mis-information or dis-information, please call your primary FBI Albany POC or email AlbanyCyber@fbi.gov. It's extremely important that FBI receive these leads quickly as we lead an interagency team with direct connectivity to national and international social media applications. In situations like these, we communicate the intelligence we have to the social media applications in an effort to combat foreign influence. Our Foreign Influence Task Force works with both our domestic and international partners to understand malign influence operations and form a unified strategy to address them.
- Fifth, monitor your networks and report any suspicious activity to us here at the FBI. Understanding new malware signatures, indicators of compromise and TTPs in real-time is extremely important for all of us.

And finally, if you do unfortunately suffer a compromise, call us immediately. I cannot overemphasize how much speed of reporting matters, especially when it comes to a potential cyber-attack initiated by Russia or its sympathizers.