BRIEFING ROOM

FACT SHEET: Act Now to Protect Against Potential Cyberattacks

MARCH 21, 2022 • STATEMENTS AND RELEASES

The Biden-Harris Administration has warned repeatedly about the potential for Russia to engage in malicious cyber activity against the United States in response to the unprecedented economic sanctions we have imposed. There is now evolving intelligence that Russia may be exploring options for potential cyberattacks.

The Administration has prioritized strengthening cybersecurity defenses to prepare our Nation for threats since day one. President Biden's Executive Order is modernizing the Federal Government defenses and improving the security of widely-used technology. The President has launched public-private action plans to shore up the cybersecurity of the electricity, pipeline, and water sectors and has directed Departments and Agencies to use all existing government authorities to mandate new cybersecurity and network defense measures. Internationally, the Administration brought together more than 30 allies and partners to cooperate to detect and disrupt ransomware threats, rallied G7 countries to hold accountable nations who harbor ransomware criminals, and taken steps with partners and allies to publicly attribute malicious activity.

We accelerated our work in November of last year as Russian President We accelerated our work in November of last year as Russian President Vladimir Putin escalated his aggression ahead of his further invasion of Ukraine with extensive briefings and advisories to U.S. businesses regarding potential threats and cybersecurity protections. The U.S. Government will continue our efforts to provide resources and tools to the private sector, including via CISA's Shields-Up campaign and we will do everything in our power to defend the Nation and respond to cyberattacks. But the reality is that much of the Nation's critical infrastructure is owned and operated by the private sector and the private sector must act to protect the critical services on which all Americans rely.

We urge companies to execute the following steps with urgency:

- Mandate the use of multi-factor authentication on your systems to make it harder for attackers to get onto your system;
- Deploy modern security tools on your computers and devices to continuously look for and mitigate threats;
- Check with your cybersecurity professionals to make sure that your systems are patched and protected against all known vulnerabilities, and change passwords across your networks so that previously stolen credentials are useless to malicious actors;
- Back up your data and ensure you have offline backups beyond the reach of malicious actors;
- Run exercises and drill your emergency plans so that you are prepared to respond quickly to minimize the impact of any attack;
- Encrypt your data so it cannot be used if it is stolen;
- Educate your employees to common tactics that attackers will use over email or through websites, and encourage them to report if their computers or phones have shown unusual behavior, such as unusual crashes or operating very slowly; and
- Engage proactively with your local FBI field office or CISA Regional Office to establish relationships in advance of any cyber incidents. Please encourage your IT and Security leadership to visit the websites of CISA and the FBI where they will find technical information and other useful resources.

We also must focus on bolstering America's cybersecurity over the long term. We encourage technology and software companies to:

- Build security into your products from the ground up — "bake it in, don't bolt it on" — to protect both your intellectual property and your customers' privacy.
- Develop software only on a system that is highly secure and accessible only to those actually working on a particular project. This will make it much harder for an intruder to jump from system to system and compromise a product or steal your intellectual property.
- Use modern tools to check for known and potential vulnerabilities. Developers can fix most software vulnerabilities — if they know about them. There are automated tools that can review code and find most coding errors before software ships, and before a malicious actor takes advantage of them.

- Software developers are responsible for all code used in their products, including open source code. Most software is built using many different components and libraries, much of which is open source. Make sure developers know the provenance (i.e., origin) of components they are using and have a "software bill of materials" in case one of those components is later found to have a vulnerability so you can rapidly correct it.

- Implement the security practices mandated in the President's Executive Order, *Improving our Nation's Cybersecurity*. Pursuant to that EO, all software the U.S. government purchases is now required to meet security standards in how it is built and deployed. We encourage you to follow those practices more broadly.

###