U.S. COMMODITY FUTURES TRADING COMMISSION
Three Lafayette Centre
1155 21st Street, NW, Washington, DC 20581
Telephone: (202) 418-5000

Market Participants
Division

Amanda L. Olear
Acting Director

December 17, 2021

Greetings:

The White House and the Department of Homeland Security Cyber and Infrastructure Security Agency just issued some significant alerts noting the importance of heightened vigilance concerning cybersecurity both during and after the holiday period, and the importance of focusing on cybersecurity in the current threat environment. We are forwarding these to you to emphasize that it would be advisable and appropriate for you to promptly review these alerts, to take the immediate risk mitigation steps they address, and to maintain heightened cybersecurity alertness as 2022 begins.

Best regards,

Clark Hutchison, Director, Division of Clearing and Risk
Meghan Tente, Acting Director, Division of Market Oversight
Amanda Olear, Acting Director, Market Participants Division

You are subscribed to National Cyber Awareness System Current Activity for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available. [***NOTE: the Divisions urge you to subscribe to this source if you have not done so already***]

Immediate Steps to Strengthen Critical Infrastructure against Potential Cyberattacks

12/15/2021 08:10 AM EST

Original release date: December 15, 2021

In light of persistent and ongoing cyber threats, CISA urges critical infrastructure owners and operators to take immediate steps to strengthen their computer network defenses against potential cyberattacks. CISA has released CISA Insights: Preparing For and Mitigating Potential Cyber Threats to provide critical infrastructure leaders with steps to proactively strengthen their organization's operational resiliency against sophisticated threat actors, including nation-states and their proxies.

CISA encourages leadership at all organizations—and critical infrastructure owners and operators in particular—to review the CISA Insights and adopt a heighted state of awareness.

Protecting Against Malicious Cyber Activity before the Holidays

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology and Chris Inglis, National Cyber Director

SUBJECT: Protecting Against Malicious Cyber Activity before the Holidays

DATE: December 16, 2021

The holidays are an opportunity to spend time with our loved ones and enjoy some well-earned rest. Unfortunately, malicious cyber actors are not taking a holiday – and they can ruin ours if we're not prepared and protected. Historically we have seen breaches around national holidays because criminals know that security operations centers are often short-staffed, delaying the discovery of intrusions. Beyond the holidays, though, we've experienced numerous recent events that highlight the strategic risks we all face because of the fragility of digital infrastructure and the ever- present threat of those who would use it for malicious purposes.

There are specific steps that you, as leaders, can initiate now to reduce the

risk of your organizations during this time of heightened risk and into the New Year.

Below are some recommendations for actions you can take immediately to have an incident-free holiday season.

Ensuring a Cyber Safe and Secure Holiday Season

In many cases criminals plan and actually begin an intrusion before the holiday itself – they infiltrate a network and lie in wait for the optimal time to launch an attack. It is therefore essential that you convene your leadership team now to make your organization a harder target for criminals.

Here are some best practices that can be implemented immediately. We recommend that you confirm with your IT teams that these are in place:

- **Updated Patching**. Criminals count on victims failing to patch their systems and usually take advantage of long-known and fixable vulnerabilities. Patching should be up-to-date, against all known vulnerabilities.

- **Know your Network**: Enable logs; pay attention; investigate quickly. Intrusions can be stopped before the impact. Secure organizations assume they will be compromised, but work to minimize the effect of a compromise.

- **Change Passwords and Mandate Multi-Factor Authentication (MFA)**. Ask your IT staff how long it has been since employees changed their passwords. Many criminals use stolen credentials, so forcing a reset (with adequate length and complexity) before the holidays can deny malicious actors access to your systems. At the same time, confirm that your organization has implemented MFA and that it is required without exception. If you have MFA available, but are not requiring it, change that – require all staff to use the security technology that you have already acquired. MFA significantly reduces your risk from almost all opportunistic attempts to gain entry into key systems.

- **Manage Schedules**. Review staffing plans for your IT and security teams to ensure you have sufficient holiday coverage. Similarly, identify those IT and security employees who are on 24/7 call in the event of a cybersecurity incident or ransomware attack. Minutes count in the event of an attack and any delays in response typically magnify the consequences of a successful attack. Having current, validated information and a plan to reach out is critical.

- **Employee Awareness**. Conduct spear phishing and other exercises to raise employee awareness of common attacks. Reinforce the imperative to report computers or phones exhibiting any unusual behavior. Deny the criminals the initial entry into your systems that allows them to execute attacks over the

holidays and beyond.

- **Exercise Makes an Organization Healthy**. Exercise your incident response plan now, so that if the worst happens you can respond quickly to minimize the impact. Conducting rigorous security stress tests now also gives you time to make needed improvements or to develop a basic plan if you do not have one.

- **Back up your Data**. Confirm that you are backing up key data. Ask your IT staff to test the backup system, and verify that that these backups are offline and COMPLETELY out of the reach of criminals. Many attacks succeed simply because the organizational back-up strategy is incomplete or permits criminals access to the backed-up information.

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.

All of us can, and must, play a part to improve the Nation's cybersecurity. The U.S. government and the private sector have accomplished much together in the past year, and we have much more to do in 2022 and beyond.

Please accept our best wishes for a happy holiday season and a safe and secure New Year.