OFFICES OF HOMELAND SECURITY AND CIVIL DEFENSE
Inasiguran I Tano' Guahan/Ufisinan Difensia Sibet
221-B Chalan Palasyo, Agana Heights, Guam 96910
Tel: (671) 475-9600 / Fax: (671) 477-3727
Website: www.ghs.guam.gov

Samantha J. Brennan
Homeland Security Advisor
Charles V. Esteves
Administrator

For Immediate Release
March 4, 2022

GHS/OCD and MRFC Recommend Strengthened Cybersecurity for Organizations

In light of the Russian incursion into Ukraine and informed by the Mariana Regional Fusion Center (MRFC), U.S. Department of Homeland Security (DHS) counterparts and other key partners, the Offices of Guam Homeland Security and Civil Defense (GHS/OCD) recommends organizations in Guam consider strengthening their cybersecurity postures to mitigate possible cyber-attacks.

In recent years, Russian state sponsored malicious cyber activities ranged from online malign influence campaigns, denial of service attacks, website defacements, ransomware, and cyber espionage. State sponsored malicious cyber activities affected industries and infrastructure across a broad spectrum to include COVID-19 responses and research, government agencies, healthcare, energy, commercial facilities, manufacturing, supply chains, and economic sectors.

The Russian Government and its proxies utilized cyber activities as a key component of their force projection over the last decade and recognizes striking critical infrastructure operations may apply pressure to a country's government, military, and population. Russian actors conducting malicious cyber activities were linked with several operationally and economically damaging events to include the 2020 compromise of the SolarWinds software, targeting of U.S. companies developing COVID-19 vaccines, the 2018 targeting of U.S. industrial control system infrastructure, NotPetya ransomware, and the 2016 leaks of documents stolen from the U.S. Democratic National Committee.

GHS/OCD and MRFC recommend the following cybersecurity precautions be observed during this time of heightened tensions:

- **Report suspicious network activity or suspected malicious cyber activity to the agency's network administrators and the MRFC at (671) 475-0400 or via email at mrfc@ghs.guam.gov.**
- Ensure that software is up to date, prioritizing updates that address known vulnerabilities.
- Confirm that the organization's entire network is protected by up-to-date antivirus/antimalware software.
- Keep backups and test backup protocols and procedures; ensure that backups are isolated from network connections.
- Validate all remote access to the organization's network.
- Utilize multi-factor authentication.
- Inform cybersecurity/IT personnel to be vigilant and focused on identifying any unexpected or unusual network behavior.
- Enable event logging, to better investigate issues or events.

Additional tips and best practices available to the public may be accessed at the U.S. DHS's Cybersecurity and Infrastructure Security Agency webpage at https://www.cisa.gov.

The MRFC serves as the local hub of information sharing and suspicious incident coordination for Guam and the Northern Mariana Islands. If you observe any suspicious network activity, please contact the MRFC at (671) 475-0400 or via email at mrfc@ghs.guam.gov.

-###-