



***Joint Message from the Federal Bureau of Investigation and the
Cybersecurity and Infrastructure Security Agency***



March 6, 2022

Partners,

From the outset of Russia's threat to Ukraine's sovereignty, the FBI and DHS have engaged daily in efforts to support the U.S. response and to secure the homeland from potential impacts related to the Russia-Ukraine crisis. DHS has been designated as the lead Federal agency to coordinate domestic preparedness and response efforts related to the current crisis. DHS has established a Unified Coordination Group (UCG) to ensure unity of effort across the Federal Government in preparing for and responding to possible related threats to the homeland; develop and pursue strategic objectives and priorities; and coordinate with Federal, state, local, tribal, and territorial officials, as well as representatives of the private sector and nongovernmental entities in support of these objectives and priorities. The FBI is a member of this UCG and will continue to respond to all cyber incidents and work with DHS to share actionable, timely, and valuable intelligence arising from this unfolding situation that may affect you and your areas of responsibility.

While Russia is already engaged in cyber-attacks aimed at Ukraine, the FBI and DHS are concerned about potential cyberattacks or spillover to organizations within the United States. While there is no specific, credible threat to the U.S. homeland at this time, the FBI and DHS, along with their partners, continue to monitor the threat environment 24/7.

The FBI will continue to post information and alerts regarding cyber and other threats for law enforcement partners to the Law Enforcement Enterprise Portal (LEEP) as they become available. Cyber threat and network defense information can also be found at the FBI's [Internet Crime Complaint Center \(IC3\)](#). Similarly, DHS will also ensure the latest products and information are made available via the [Homeland Security Information Network \(HSIN\)](#).

The Cybersecurity and Information Security Agency (CISA) continues working with organizations across every sector to strengthen the cybersecurity of our networks and infrastructure. CISA launched Shields Up – www.cisa.gov/shields-up – a central web page with regularly updated guidance to help organizations understand the changing threat landscape and adopt a stronger cybersecurity posture. In the event of a cyber incident, FBI and CISA can help victims and use information from incident reports to help prevent other similar intrusions, and ensure that we can take critical actions to mitigate risk. All organizations should report incidents and anomalous activity to CISA's 24/7 Operations Center at central@cisa.dhs.gov or (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Please share this communication with your law enforcement partners and encourage them to maintain open lines of communication with their local FBI field offices and/or Joint Terrorism Task Forces, deployed DHS Intelligence Officers, and CISA regional cybersecurity personnel.

Thank you again for your continued partnership.

Paul Abbate
Deputy Director
Federal Bureau of Investigation

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency