ALERT

Cleared Defense Contractors at Risk from Russian Cyber Activity; Advisory Shows Government Expectations

February 17, 2022

What: Cleared Defense Contractors (CDCs) are being actively targeted by Russian state-sponsored cyber activity, according to a Joint Cybersecurity Advisory from the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) published on February 16, 2022. Large and small CDCs and subcontractors with varying levels of cybersecurity resources are being preyed upon as Russian actors seek sensitive U.S. defense information and technology.

What does it mean for industry: With the pace of public warnings and recommended actions increasing, private companies are on notice about government expectations for cybersecurity prevention and mitigation. Here, Russian actors are actively working to steal sensitive information from companies that support the U.S. military and intelligence community. Targeted industries include those involved with weapons and missile development, vehicle and aircraft design, software development and information technology, data analytics, and logistics. The government is telling the private sector (both prime contractors and their numerous subcontractors) that malicious cyber actors have acquired sensitive, unclassified information, as well as CDC-proprietary and export-controlled technology, to obtain significant insight into U.S. weapons platforms development and deployment timelines, vehicle specifications, and plans for communications infrastructure and information technology.

The U.S. government has provided numerous warnings about Russian state-sponsored cyber activity over the past year. In the context of Russia's continued threatening behavior towards Ukraine, CISA has

Authors

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersecurity

Government Contracts

Privacy, Cyber & Data Governance

recently focused on communicating threats to critical infrastructure that could disrupt essential services. Russian state-sponsored malicious cyber actors are known to rely on "common but effective" techniques to gain access to CDC networks, maintain persistence, and exfiltrate data. The cybersecurity advisory explains the nature of the threat and actions companies can take to protect against this kind of malicious cyber activity. Companies should pay particular attention to the recommended actions.

What does the Advisory say?

FBI, NSA, and CISA warn that Russian state-sponsored cyber actors have been targeting U.S. CDCs for the last 2 years. Compromised entities have included CDCs supporting the U.S. Army, U.S. Air Force, U.S. Navy, U.S. Space Force, and U.S. Department of Defense (DOD) and intelligence programs. These threat actors have exfiltrated hundreds of documents related to the companies' products, relationships with other countries, and internal personnel or legal matters. The government says that theft of this information from CDCs has given Russian threat actors significant insight into U.S. weapons platforms development and deployment timelines, plans for communications infrastructure, and specific technologies employed by the U.S. government and military. Contractors large and small supporting the U.S. military and intelligence community have been victimized, with particular focus in the following areas:

- Command, control, communications, and combat systems;
- Intelligence, surveillance, reconnaissance, and targeting;
- Weapons and missile development;
- Vehicle and aircraft design; and
- Software development, data analytics, computers, and logistics.

The "common but effective" tactics that have gained access to target networks include "spearphishing, credential harvesting, brute force/password spray techniques, and known vulnerability exploitation against accounts and networks with weak security. These actors take advantage of simple passwords, unpatched systems, and unsuspecting employees to gain initial access before moving laterally through the network to establish persistence and exfiltrate data." The government says that recently, Russian actors have prioritized the Microsoft 365 environment. The advisory summarizes malicious activity across multiple phases:

- Initial access;
- Credential access;
- Collection; and
- Command and Control.

Finally, FBI, NSA, and CISA offer detection and remediation recommendations. To detect malicious activity, the advisory continues to recommend a combination of technological and operational cybersecurity activities to detect unusual activity and look for indicators of known Tactics, Techniques, and Procedures (TTPs). Recommended mitigations include:

- Enforce multifactor authentication.
- Enforce strong, unique passwords.
- Enable M365 Unified Audit Logs.
- Implement endpoint detection and response tools.

This type of malicious cyber activity is expected to increase as tensions rise over Russia's potential invasion of Ukraine.

Key Takeaways

Wiley has been advising companies in the technology and government contracting space for years to take a risk-management approach to building reasonable cybersecurity programs. We encourage cleared defense contractors to take the mitigation actions outlined in the advisory if they have not done so already. In addition to the inherent operational and business risk posed by these cyber actors, the U.S. government has continued to set expectations that cleared defense contractors enhance their cybersecurity posture and "adapt to the continuously changing threat environment." These expectations extend to subcontractors as well, in light of the government's oft-stated concerns about supply chain security and visibility into cybersecurity. And ideally, the government would like all contractors and companies across the economy to elevate their approach to cybersecurity.

In the absence of comprehensive federal law or applicable sector-specific requirements, companies of all types can look to federal contracting standards, the National Institute of Standards and Technology (NIST) publications, industry best practices, and other "soft law" to build effective and defensible programs. Such programs must iterate in response to new threats and the increasing regulatory risk from federal and state government action.

Companies need to be proactive to help protect against litigation, oversight, and potential civil fraud enforcement. We recommend reviewing relevant cybersecurity requirements and publications like the Joint Cybersecurity Advisory, and incorporating government guidance into risk management plans. We encourage all organizations to consider how their information security procedures compare to these evolving expectations, as senior government officials continue to emphasize that they expect companies to follow the government's lead in improving cyber readiness.

To learn more about cyber readiness and rapidly-evolving government expectations, or for help dealing with a cyber incident, feel free to contact any of the authors listed.