**Steven Pelak**

Partner
202.654.6929
Washington, D.C.
swpelak@hollandhart.com

**Matthew Cavarra**

Partner
303.295.8169
Denver
mncavarra@hollandhart.com

# DOJ Settlement Sets Forth Best Practices for Protecting Sensitive Data for Government Contractors and Information Technology Companies

**Publication — January 2018**

If your company sells products or services to the U.S. Department of Defense or intelligence community, you should be aware of the cybersecurity best practices set forth in the U.S. Department of Justice's ("DOJ") recent Non-Prosecution Agreement with Netcracker Technology Corporation ("Netcracker"), a U.S.-based global telecommunications software company.

Citing the growing cyber threat posed by foreign government security agencies and cyber criminals, the U.S. Government is leaning on its government contractors to take appropriate measures to safeguard sensitive government information stored on non-governmental networks and systems, including adopting security plans that limit the information sent to, stored in, or accessed from outside the United States. For example, effective December 31, 2017, government contractors handling sensitive federal government information must now comply not only with the cyber compliance requirements in Defense Federal Acquisition Regulation Supplement ("DFARS") 252.204-7012, but also with the National Institute of Standards and Technology ("NIST") Special Publication 800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. The DOJ's enforcement action against Netcracker offers valuable insight into the types of enhanced cybersecurity protocols that the U.S. Government expects government contractors to adopt. Non-DOD agencies have required a lesser compliance standard since June of 2016 under Federal Acquisition Regulation ("FAR") 4.19 and 52.204-21, but non-DOD contractors can expect a migration to the tougher standards in the future.

On December 11, 2017, the DOJ announced its non-prosecution agreement with Netcracker, which is a wholly owned subsidiary of Japan-based NEC Corp. This settlement resolved allegations that Netcracker allowed employees located in Russia and Ukraine who lacked security clearances to perform software customization and configuration services under a federal contract with the U.S. Defense Information Systems Agency ("DISA"). As a part of the settlement, Netcracker agreed to implement, and share with others in the industry, enhanced cybersecurity measures for software development, implementation, and other services to its U.S.-based clients. In 2015, Netcracker agreed to pay $11.4 million to settle related civil allegations under the False Claims Act that the company used foreign nationals without security clearances to work on a DISA contract.

According to the Non-Prosecution Agreement's Statement of Facts, Netcracker worked as a subcontractor on two government contracts with

DISA and allegedly allowed Netcracker personnel in Russia and Ukraine to have access to DISA information and perform software services under one of the contracts during 2008 through 2013. The software at issue was one of Netcracker's commercial off-the-shelf ("COTS") products. Although Netcracker had certified that all employees assigned to this project would be U.S. citizens and have a security clearance of Secret or above, Netcracker and DISA had different understandings of the term "project" and what constituted "DISA information." The company believed it could use uncleared employees, including foreign nationals outside of the United States, to work on the DISA project as long as the employees did not have access to classified or sensitive information.

DOJ's investigators determined that DISA project source code and other information was stored on a Netcracker server in Moscow and that uncleared Netcracker employees in Russia and Ukraine knew they were customizing and configuring sensitive software code for the DISA project. Netcracker's actions not only may have violated U.S. export control laws, but also potentially made federal government networks vulnerable to foreign surveillance. According to the Statement of Facts, any DISA data sent to Russia and/or transferred over Russian networks via Netcracker's servers were subject to the Russian System of Operative-Investigative Measures, which authorizes the Federal Security Service of the Russian Federation to collect, analyze, and store both metadata and content transmitted or received on Russian telecommunication networks.

To avoid criminal prosecution, Netcracker agreed to create an Enhanced Security Plan for U.S.-based customers' domestic communications infrastructure. The plan includes the following key features:

- The company must appoint a Security Director approved by the DOJ who has a security clearance of at least Top Secret;
- Netcracker must agree to keep specified data and information in the United States, and move its file storage and servers to the United States;
- Netcracker cannot transfer or route certain sensitive data outside the United States; and
- The company must move certain supervisory jobs, including management of employee screening, to the United States.

Although Netcracker appears to have avoided criminal liability in this instance, one might reasonably conclude that the costs in time and money of the resulting internal investigation and added security measures were substantial. The Netcracker matter serves as an important reminder to ensure all persons working on government defense or intelligence contracts have appropriate authorization and security clearances. Particularly where you are providing any goods or services to another private contractor, you should obtain appropriate assurances regarding (a) the U.S. person status of any persons employed by or working on behalf of the other private contractor, or (b) the licensed/authorization status under applicable export control laws of any foreign persons employed by or working on behalf of the other private contractor. As the U.S. Government has made clear in prior enforcement actions, you should take these steps

even if your company is supplying the U.S. Department of Defense or intelligence community with non-classified COTS products and related services as in the Netcracker matter.

Holland & Hart's Export Control/Trade Sanctions, Cybersecurity, and Government Contracts teams have extensive experience in assisting U.S. and non-U.S. clients in due diligence and internal investigation efforts, including those arising in the merger and acquisition context as such issues are considered in evaluating or assessing contractual assets and liabilities. If you have any questions about the topics discussed in this Client Alert or we may assist you in dealing with due diligence, internal investigations, or investigations or enforcement actions by the U.S. Government, please contact the following Holland & Hart lawyers: Export Controls/Trade Sanctions: Steven Pelak and Jason Prince; Cyber/Privacy Law: Romaine Marshall; and Government Contracts/IP Licensing: Charles Lucy and Matthew Cavarra. Whether the legal assistance needed is small or large or best serviced by an individual lawyer or a team, we have nationally recognized lawyers with deep governmental and private industry experience available to assist you from Alaska to Washington, D.C., from Utah to Colorado, and from Idaho to Nevada.