THE
NATIONAL LAW REVIEW

DOJ Settlement with Netcracker Technology Corporation Highlights Cybersecurity and Export Control Best Practices for Government Contractors and Information Technology Companies

Thursday, December 14, 2017

Article By Drinker Biddle & Reath LLP
Nate BolinDBR on Data

Labor & Employment
Government Contracts, Maritime & Military Law
Communications, Media & Internet
All Federal

This week the U.S. Department of Justice (DOJ) and Netcracker Technology Corporation (NTC) announced that they had settled charges that NTC had violated U.S. controls on foreign access to sensitive data. The settlement underscores many of the export control and related compliance risks surrounding the provision and use of cloud computing services and global networks. At the same time, the Enhanced Security Plan issued by NTC and DOJ as part of the settlement provides a helpful set of benchmarks and best practices for companies that may be considering the use of cloud services and network infrastructure to house and transmit their most sensitive data.

According to DOJ's settlement announcement, NTC had worked as a subcontractor on two federal government contracts with the Defense Information Systems Agency (DISA), a combat support agency of the U.S. Department of Defense (DoD), and performed some product support work from locations outside the United States, including Russia. DOJ alleged that by failing to maintain adequate controls on the cloud and network infrastructure supporting these contracts, NTC had threatened the security of sensitive data about individuals, DoD projects, networks and critical U.S. domestic communications infrastructure. DOJ further asserted that uncleared NTC foreign national employees in Russia and Ukraine worked on the DISA projects and were aware of the sensitive nature of the projects and the data stored and transmitted through the network managed by DISA.

U.S. law imposes a number of restrictions on the storage, transmission and use of data on cloud services and international data networks. The U.S. Export Administration Regulations (EAR) and U.S. International Traffic in Arms Regulations (ITAR) require licenses and other forms of government authorization before foreign persons may handle, transmit or access certain controlled software, technology or technical data. For example, cloud service providers and network infrastructure companies that hire foreign employees may need licenses from the Directorate of Defense Trade Controls (which oversees the ITAR) or the Bureau of Industry and Security (which enforces the EAR) before those employees can access their systems. For some sensitive data – such as sensitive technical data related to defense articles controlled by the ITAR – simply transmitting or storing the data overseas can result in a violation of the ITAR. Under current ITAR rules, this is true even if the data themselves are encrypted from end to end.

Companies providing cloud and data services to the U.S. government as well as prime contractors and subcontractors receiving U.S. government funding must comply with federal acquisition rules governing the handling, storage and transmission of various categories of "controlled" information. In certain cases, these rules may require the reporting of unauthorized releases and cybersecurity breaches within 72 hours.

The Enhanced Security Plan issued by DOJ and NTC identifies a number of key internal policies and procedures that can be implemented to meet these requirements, including:

- Setting the "tone at the top" by appointing a senior corporate officer as the director of cloud and network

security, with the appropriate credentials and background to understand and institute proper information handling and security procedures.

- Developing and implementing a detailed security policy governing user access, systems monitoring and personnel screening.
- Authenticating and tracking changes to systems software through code-signing and other means.
- Restricting access, transmission and storage of certain sensitive data to U.S.-based servers and U.S.-based network infrastructure.
- Controlling access by non-U.S. persons and implementing procedures for the proper vetting and licensing of non-U.S. employees and agents.
- Conducting periodic third-party audits of the security procedures and their implementation.

Companies doing business with the U.S. government or handling or using export-controlled technology, software, technical data, and cloud and network services should review these policies and procedures and consider whether to include them in their own compliance programs.

Source URL: https://www.natlawreview.com/article/doj-settlement-netcracker-technology-corporation-highlights-cybersecurity-and-export