



Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, APRIL 10, 2014
WWW.JUSTICE.GOV

AT
(202) 514-2007
TTY (866) 544-5309

JUSTICE DEPARTMENT, FEDERAL TRADE COMMISSION ISSUE ANTITRUST POLICY STATEMENT ON SHARING CYBERSECURITY INFORMATION

Sharing Cyber Threat Information Can Help Secure Nation's Networks and Improve Efficiency; Properly Designed Sharing Not Likely to Raise Antitrust Concerns

WASHINGTON – The Department of Justice and the Federal Trade Commission (FTC) today issued a [policy statement on the sharing of cybersecurity information](#) that makes clear that properly designed cyber threat information sharing is not likely to raise antitrust concerns and can help secure the nation's networks of information and resources. The policy statement provides the agencies' analytical framework for information sharing among private entities and is designed to reduce uncertainty for those who want to share ways to prevent and combat cyberattacks.

“The Department of Justice is committed to doing all it can to protect the security of our nation's networks. Through the FBI and the National Security and Criminal Divisions, the department plays a critical role in preventing and prosecuting cybercrime,” said Deputy Attorney General James M. Cole. “Private parties play a critical role in mitigating and responding to cyber threats, and this policy statement should encourage them to share cybersecurity information.”

“Cyber threats are increasing in number and sophistication, and sharing information about these threats, such as incident reports, indicators and threat signatures, is something companies can do to protect their information systems and help secure our nation's infrastructure,” said Assistant Attorney General Bill Baer in charge of the Department of Justice's Antitrust Division. “With proper safeguards in place, cyber threat information sharing can occur without posing competitive concerns.”

“Because of the FTC's long experience promoting data security, we understand the serious threat posed by cyberattacks,” said FTC Chairwoman Edith Ramirez. “This statement should help private businesses by making it clear that antitrust laws do not stand in the way of legitimate sharing of cybersecurity threat information.”

In the policy statement, the federal antitrust agencies recognize that the sharing of cyber threat information has the potential to improve the security, availability, integrity and efficiency of the nation's information systems. The policy statement also emphasizes that the legitimate sharing of cyber threat information is very different from the sharing of competitively sensitive information such as current or future prices and output or business plans, which may raise antitrust concerns. Cyber threat information is typically technical in nature and covers a limited type of information, and disseminating that information appears unlikely to raise competitive concerns.

The joint Department of Justice/Federal Trade Commission “Antitrust Guidelines for Collaborations Among Competitors” provide an overview of the agencies’ analysis of information sharing as a general matter. The agencies consider whether the relevant agreement likely harms competition by increasing the ability or incentive to raise price above or reduce output, quality, service or innovation below what likely would prevail in the absence of the relevant agreement.

Previous antitrust analysis on cyber threat information sharing was issued in October 2000, when the Antitrust Division issued specific guidance in a [business review letter to Electric Power Research Institute Inc.](#) Under the Justice Department’s business review procedure, an organization may submit a proposed action to the Antitrust Division and receive a statement as to whether the division will challenge the action under the antitrust laws. In that letter, the Antitrust Division confirmed that it had no intention of taking enforcement action against the company’s proposal to exchange certain cybersecurity information, including exchanging actual real-time cyber threat and attack information. In that matter, the division concluded that as long as the information exchanged was limited to physical and cybersecurity issues, the proposed interdictions on price, purchasing and future product innovation discussions should be sufficient to avoid any threats to competition. The legal analysis in that matter remains current.

#

14-365

MEDIA CONTACT: Gina Talamona
Department of Justice
Office of Public Affairs
202-514-2007

Peter Kaplan
Federal Trade Commission
Office of Public Affairs
202-326-2180