



# Department of Justice

FOR IMMEDIATE RELEASE  
THURSDAY, APRIL 10, 2014  
[WWW.JUSTICE.GOV](http://WWW.JUSTICE.GOV)

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

**REMARKS AS PREPARED FOR DELIVERY BY ASSISTANT ATTORNEY  
GENERAL BILL BAER AT THE PEN AND PAD BRIEFING ON THE  
JUSTICE DEPARTMENT AND FEDERAL TRADE COMMISSION JOINT  
ANTITRUST POLICY STATEMENT ON SHARING OF CYBERSECURITY  
INFORMATION**

WASHINGTON, D.C.

Good afternoon and thanks for joining us. Thank you Rand for all you, Lisa Monaco and your team do every day to keep Americans safe. Jim, thank you as always for your leadership on cyber security issues at the department. And thanks to Edith Ramirez and the FTC for being our long time partners in protecting consumers and competition and providing clear guidance to the business community on antitrust issues.

As Rand and Jim just mentioned, today the Department of Justice and the Federal Trade Commission issued a joint antitrust policy statement on the sharing of cybersecurity information. We all recognize the critical importance of protecting our nation's networks. And we also know that this can be done in legitimate and lawful ways.

This is an antitrust no-brainer: Companies who engage in properly designed cyber threat information sharing will not run afoul of the antitrust laws. This means that as long as companies don't discuss competitive information such as pricing and output when sharing cybersecurity information, they're okay.

As we are well aware, cyber threats are increasing in number and sophistication, and sharing information about 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. This kind of information sharing is good public policy. And the antitrust agencies support it.

That is why DOJ and the FTC are issuing today's statement. If there ever was any uncertainty out there about the kind of information that can be shared, this policy statement should make it abundantly clear that with the proper safeguards in place, cyber threat information sharing can occur without antitrust risk.

We are committed to providing clarity and transparency about our antitrust enforcement principles. We do that in many ways, including the Antitrust Division's business review process.

Under that procedure, an organization can talk to us about a proposed action and its potential antitrust implications and receive a written statement from us as to whether the division intends to challenge the action under the antitrust laws.

Indeed, in 2000, the Antitrust Division issued just such a letter on a proposal involving cybersecurity information sharing, concluding that it had no intention of taking enforcement action against a research institute'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, and avoided delving into antitrust-sensitive issues such as price, purchasing and future product innovation, we saw no issue from an antitrust perspective.

Today's statement confirms that the legal analysis in that business review letter remains the current enforcement policy of the United States antitrust enforcement agencies. And we stand ready to engage with the business community going forward to make sure they can continue to cooperate to protect our nation's security and the interests of its consumers.

And now I am happy to turn it over to my good friend, FTC Chairwoman Edith Ramirez.

###