THE UNITED STATES DEPARTMENT of JUSTICE
STICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, October 6, 2021

Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

Deputy Attorney General Lisa O. Monaco announced today the launch of the department's Civil Cyber-Fraud Initiative, which will combine the department's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.

"For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it," said Deputy Attorney General Monaco. "Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk. This is a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust."

The creation of the Initiative, which will be led by the Civil Division's Commercial Litigation Branch, Fraud Section, is a direct result of the department's ongoing comprehensive cyber review, ordered by Deputy Attorney General Monaco this past May. The review is aimed at developing actionable recommendations to enhance and expand the Justice Department's efforts against cyber threats.

Civil Cyber-Fraud Initiative Details

The Civil Cyber-Fraud Initiative will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients. The False Claims Act is the government's primary civil tool to redress false claims for federal funds and property involving government programs and operations. The act includes a unique whistleblower provision, which allows private parties to assist the government in identifying and pursing fraudulent conduct and to share in any recovery and protects whistleblowers who bring these violations and failures from retaliation.

The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches. The benefits of the initiative will include:

- Building broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners.
- Holding contractors and grantees to their commitments to protect government information and infrastructure.
- Supporting government experts' efforts to timely identify, create and publicize patches for vulnerabilities in commonly-used information technology products and services.
- Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.
- Reimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations.
- Improving overall cybersecurity practices that will benefit the government, private users and the American public.

The department will work closely on the Initiative with other federal agencies, subject matter experts and its law enforcement partners throughout the government.

Report Cyber-Fraud

Tips and complaints from all sources about potential cyber-related fraud, waste, abuse and mismanagement can be reported by accessing the webpage of the Civil Division's Fraud Section, which can be found here.

Topic(s):
Cyber Crime

Component(s):
Civil Division
Office of the Deputy Attorney General

Press Release Number:
21-971

Updated October 6, 2021