



Office of the Attorney General  
Washington, D. C. 20530

February 16, 2018

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS

FROM: THE ATTORNEY GENERAL

SUBJECT: Cyber-Digital Task Force

The malicious use of technology poses an unprecedented threat against our nation. While computers, smart devices, and other chip-enabled machines—as well as the networks that connect them—have enriched our lives and have driven our economy, the malign use of these technologies harms our government, victimizes consumers and businesses, and endangers public safety and national security. Indeed, the scale of this cyber threat, and the range of actors that use cyber intrusions and attacks to achieve their objectives, have grown in alarming ways.

The Department of Justice remains committed to confronting cyber threats by detecting, deterring, and disrupting malicious cyber activity through the enforcement of federal law. Therefore, today, I am establishing the Department's Cyber-Digital Task Force (the Task Force). This Task Force not only will canvass the many ways that the Department already combats the global cyber threat, but also will identify how federal law enforcement can more effectively accomplish its mission in this vital and evolving area.

The Task Force shall be chaired by a senior Department official appointed by the Deputy Attorney General and shall consist of representatives from the Criminal Division; the National Security Division; the United States Attorney's Office community; the Office of Legal Policy; the Office of Privacy and Civil Liberties; the Office of the Chief Information Officer; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. The Deputy Attorney General may invite representatives from other Department components, and from other federal agencies, to participate in the Task Force as appropriate, and may establish subcommittees to focus the Task Force's efforts.

Many of the most pressing cyber threats that our nation faces transcend easy categorization. These threats include: efforts to interfere with, or disable, our critical infrastructure; efforts to interfere with our elections; use of the Internet to spread violent ideologies and to recruit followers; theft of corporate, governmental, and private information on a mass scale; use of technology to avoid or frustrate law enforcement, or to mask criminal activity; and the mass exploitation of computers, along with the weaponizing of everyday consumer devices (as well as of the very architecture of the Internet itself) to launch attacks on American citizens and businesses. Evaluating these threats, and formulating a strategy to combat them, should be among the Task Force's highest priorities.

I have asked for an initial report from the Task Force describing the Department's current cyber-related activities and offering initial recommendations by no later than June 30, 2018.

The Internet has transformed our lives. We must ensure that Internet-based technologies remain sources of enrichment, rather than becoming forces of destruction and vectors of chaos. I look forward to our continued work together in support of a prosperous and safe America.