JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051

http://oversight.house.gov

Opening Statement
Ranking Member Robin Kelly

Hearing on "Wassenaar: Cybersecurity & Export Controls"
Subcommittee on Information Technology

January 12, 2016

Thank you Mr. Chairman. Welcome to the witnesses participating in today's hearing on export controls for certain cybersecurity tools.

The export controls for intrusion and surveillance technologies agreed to at the Wassenaar Arrangement were intended to help prevent repressive regimes from obtaining and using intrusion technology against their own citizens. These are important human rights objectives. It is also critically important that U.S. cybersecurity policies advance our overall efforts to protect information and systems from cyber attacks and data breaches. Today's hearing is recognition of the fact that the federal government and private sector must work effectively together to thwart cybercrime.

The Bureau of Industry and Security's (BIS) proposed rule to implement the Wassenaar Arrangement export controls on cybersecurity intrusion and surveillance items could seriously hinder the cybersecurity industry and our national security. The language in the proposed rule would interfere with the ability of businesses and of the federal government to acquire and utilize cybersecurity tools that are critical to the security of information systems and data, and frustrate the real-time information sharing of vulnerabilities, which is relied upon to prevent or stop a cyber attack.

Going forward, BIS and its interagency partners should reconsider their policy approach to this rulemaking so that the export controls do not negatively affect our nation's ability to defend against cyber threats and the policy conforms with the broader U.S. cybersecurity strategy and national security.

The Information Technology Subcommittee has held multiple hearings examining the nature of cyber threats and how to enhance the security of information and information networks. We have learned that no company or industry is immune from cyber attacks, and cyber attackers are highly sophisticated and constantly evolving their tactics.

We are all aware of the major breaches that American companies, contractors and government agencies have sustained in recent years. Given this persistent threat to information systems, it is critically important that U.S. policies and regulations are designed to enhance the tools and capabilities that ensure the security of critical information targeted by cyber attackers.

Last month the Democratic members of this Subcommittee, along with 120 other Members of Congress, signed onto a bipartisan letter to National Security Advisor, Susan Rice, requesting the White House's collaboration and advice in the development of export control policy for cybersecurity tools. In that letter we expressed our concerns that the proposed rulemaking pertaining to export controls of intrusion software and vulnerability research could reduce the ability of private businesses and the federal government to defend against cyber threats and impair national security efforts.

I would like to commend BIS for anticipating the need to assess the impact of these export controls on the cybersecurity industry and requesting public comment on the effect of this proposed rule. The Bureau is currently reviewing the 264 public comments it received.

I look forward to hearing from today's witnesses on the impact of this proposed rule and discussing a path forward that achieves the human rights objectives of the export controls without negatively affecting innovation and research on cybersecurity tools and vulnerabilities.

Thank you, Mr. Chairman. I look forward to the witnesses' testimony.

Contact: Jennifer Hoffman, Communications Director, (202) 226-5181.