Crowell

CLIENT ALERT

To Disclose or Not To Disclose: Federal Government & Cybersecurity Vulnerabilities

November 16, 2017

On November 15, 2017, the White House Cybersecurity Coordinator, Rob Joyce, announced a formative cybersecurity policy entitled "Vulnerabilities Equities Policy and Process for the United States Government."

According to the policy, the primary focus is to "prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities discovered by the United States Government (USG)." The Vulnerabilities Equities Process (VEP) balances dissemination of vulnerability information (*e.g.*, zero day exploits) to the vendor/supplier in the expectation that it will be patched with temporarily restricting the knowledge of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence. In striking this balance, the policy aims to increase transparency regarding the process for the public and businesses, and also signals that the US will join with several countries that have announced formal policies in this area regarding management of vulnerabilities. Interestingly, this policy expands the management of vulnerabilities to include a broad array of national security and intelligence agencies.

This policy supersedes the Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process, dated February 16, 2010.

This policy applies to all USG components and personnel and contractors and includes Government off-the-shelf (GOTS), Commercial off-the-shelf (COTS), or other commercial information systems (to include open-source software), Industrial Control Systems (ICS) or products, and associated systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS).

Businesses and the public will likely be interested in the annual public reporting that is promised, which may include statistics about how many vulnerabilities go through the process and even potentially how long they are withheld from disclosure.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com

Matthew B. Welling

Partner – Washington, D.C.
Phone: +1.202.624.2588
Email: mwelling@crowell.com

Michael G. Gruden, CIPP/G
Associate – Washington, D.C.
Phone: +1.202.624.2545
Email: mgruden@crowell.com