# Executive order "promoting private sector cybersecurity information sharing": top points

Cybersecurity Law Alert

26 FEB 2015
By: Jim Halpert

In conjunction with the recent White House Summit on Cybersecurity and Consumer Protection Summit, President Barack Obama has issued a much-anticipated cybersecurity information sharing Executive Order, "Promoting Private Sector Cybersecurity Information Sharing" (EO). The purpose of the EO is to encourage the voluntary sharing of information related to cybersecurity risks and incidents between private companies, nonprofits, federal departments and agencies and other entities and to collaborate to respond to incidents "in as close to real time as possible," a lower standard than real time.

As expected, the EO – issued on February 13 – highlights the need to share information in a way that protects privacy and civil liberties, business confidentiality and the information that is shared. It also provides new parameters for the sharing of classified information by the federal government.

**White House Cybersecurity Summit**

The Summit also highlighted cybersecurity and consumer protection commitments being made by a broad group of companies. These commitments reflect the continued acceptance and use of the NIST Cybersecurity Framework by the private sector and the evolution of industry responses to the increasing number of data breaches involving personal information.

**Information sharing and analysis organizations under the Executive Order**

The EO requires the Secretary of the Department of Homeland Security to "strongly encourage" the development of "information sharing and analysis organizations" (ISAOs), a term defined in the Critical Infrastructure Information Act of 2002. The ISAOs are intended to provide a broader and more flexible means of sharing information since existing Information Sharing and Analysis Centers (ISAC) are limited by industry sector, although an ISAC could be an ISAO. The Administration anticipates that the ISAOs will be formed on a sector, subsector or regional (cross-sector) basis or in response to emerging threats and may include both public and private organizations. The White House Fact Sheet on the EO states an ISAO could also be an individual company sharing information among customers or partners. White House officials have also stated that organizations and companies that already share information will be ISAOs.

The Secretary of DHS, in consultation with other federal cybersecurity agencies, is required to enter into an agreement with a non-governmental organization for the development of a common set of voluntary standards and guidelines for ISAOs. The standards and guidelines are required to facilitate automated sharing. The standards will represent "baseline capabilities" for ISAOs in the areas of contractual agreements, operating procedures, technical means of sharing, and privacy protections. Minimization is specifically identified and is intended to cover the removal of personal information by private sector entities prior to sharing.

In developing the standards and guidelines, the organization is required to solicit public input including from organizations already engaged in information sharing, critical infrastructure owners and operators, agencies, and other stakeholders. The standards are required to be consistent with voluntary international standards to the extent those standards are consistent with the EO.

The White House Fact Sheet on the EO states that the ISAO framework is intended to provide a foundation for targeted liability protections through legislation, specifically the January 2015 White House proposal on information sharing. White House officials have explained that once an ISAO self-certifies that it is following the baseline standards and guidelines, it would qualify for liability protection (if information sharing legislation is enacted). On the other hand, the self-certification will also provide a mechanism under existing law (presumably Section 5 of the FTC Act) for a person harmed to seek redress against the ISAO.

**Critical infrastructure protection**

The EO designates the National Cybersecurity and Communications Integration Center (NCCIC) as a critical infrastructure protection program, which means it may receive information on the security of critical infrastructure or protected systems. Under the Critical Infrastructure Information Act of 2002, such critical infrastructure information shared voluntarily with the NCCIC in turn qualifies for protections from FIOA, from use in civil actions if provided in good faith, from use in criminal actions and does not constitute a waiver of a trade secret. The role of the NCCIC as a civilian information sharing hub within DHS was codified by the National Cybersecurity Protection Act of 2014.

Under the EO, the NCCIC is required to enter into voluntary agreements with ISAOs on information sharing and the Secretary of Homeland Security is required to determine the eligibility of ISAOs and their members for security clearances that may be required for sharing under the voluntary agreements. The EO provides that other federal agencies with cybersecurity responsibilities including to protect public health and safety, national security and economic security from threats may participate in the activities provided for under these voluntary agreements. The NCCIC is authorized under existing law to share cyberthreat information, situational analysis and technical assistance with these federal agencies.

**Privacy and civil liberties protections**

The privacy section of the EO is limited to federal agencies. The federal agencies participating in activities under the EO are required to work with their senior agency officials on privacy and civil liberties in order to ensure that protections are adequate and are based upon the Fair Information Practice Principles[1] and other similar policies. Agencies are required to conduct assessments of these activities and report to the DHS Chief Privacy Officer and the DHS Office for Civil Rights and Civil Liberties for inclusion in the Privacy and Civil Liberties Assessment report.

**Sharing of classified information**

The federal government has significant classified information about cybersecurity threats that private sector representatives have asked to receive on a more regular basis. Toward this end, the EO requires the Secretary of Defense, with the concurrence the Secretary of Energy, the Nuclear Regulatory Commission (NRC), the Director of

National Intelligence and the Secretary of Homeland Security to develop and issue a "National Industrial Security Program Operating Manual." The portion of the manual pertaining to information classified pursuant to the Atomic Energy Act of 1954 will be prescribed by the Secretary of Energy and the NRC, the portion related to intelligence sources and methods will be prescribed by the Director of National Intelligence, and the portion related to classified information shared under a critical infrastructure protection program (ie, the NCCIC) will be prescribed by the Secretary of Homeland Security and will provide arrangements necessary to permit the sharing with authorized private sector individuals and organizations.

**Regulatory limitations**

Finally, the EO states that it shall not be interpreted to alter or limit existing law including as related to agency activities conducted with the private sector relating to criminal or national security threats. In order to assuage any potential industry concerns, the EO includes limitations language clarifying that it does not provide an agency with authority to regulate the security of critical infrastructure beyond the authority under existing law.

Find out more about these developments by contacting the authors.

---

[1] The eight Principles are set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

## AUTHORS

**Jim Halpert**
Partner
Washington, DC | T: +1 202 799 4000
jim.halpert@dlapiper.com