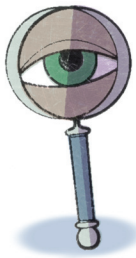
PHILLIPS LYTLE LLP CLIENT ALERT
DATA SECURITY & PRIVACY
FEBRUARY 2017



NIST Introduces Proposed Updates to Cybersecurity Framework

Companies Have Until April 10, 2017 to Comment

Recently, the National Institute of Standards and Technology ("NIST") released a proposed update ("Proposed Update") to its Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework"). This Proposed Update, if implemented, would update the February 2014 version of the Cybersecurity Framework.

For background, the Cybersecurity Framework was created through the collaborative efforts of both industry and government, and it consists of standards, guidelines and practices for private sector organizations to promote the protection of critical infrastructure, systems and networks. Although complying with the Cybersecurity Framework is voluntary, the Cybersecurity Framework provides a cyber-risk management guide that organizations can tailor to their own specific needs. The Proposed Update would not change the core functions of the Cybersecurity Framework, which include the following:

- Identify – develop the organizational understanding to manage cybersecurity risk to systems' assets, data and capabilities;
- Protect – develop and implement the appropriate safeguards to insure delivery of critical infrastructure services;
- Detect – develop and implement the appropriate activities to identify the occurrence of a cybersecurity event;
- Respond – develop and implement the appropriate activities to take action regarding a detected cybersecurity event; and
- Recover – develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

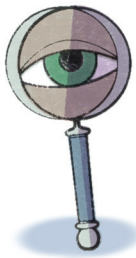
Four Key Features of the Proposed Update

1. Supply Chain Risk Management

The Proposed Update includes a section on supply chain risk management. This new section puts emphasis on the review of third parties, including vendors, suppliers and information technology providers, and the cybersecurity risks that may exist in the supply chain involving these third parties. Specifically, Section 3.3 of the Proposed Update requests that organizations (i) determine the cybersecurity requirements of third parties who can access the organization's critical infrastructure; (ii) enact appropriate cybersecurity requirements and governance with third parties via contractual arrangements; (iii) communicate with third parties as to how the organization will verify that the third parties are following their cybersecurity requirements; and (iv) verify that the cybersecurity requirements are satisfied by third parties through assessment methodologies. For example, an organization that purchases information technology equipment or services from a third party may request a Cybersecurity Framework profile, providing the purchasing organization the ability to assess the third party supplier's cybersecurity risk management procedures.

2. Information Sharing Practices

The Proposed Update also adds guidance related to information sharing practices. Through information sharing, organizations can compare their cybersecurity risk management procedures to other organizations also utilizing the guidance set forth in the Cybersecurity Framework.



3. Access Control

The updated Identity Control and Access Control section encourages organizations to implement comprehensive authentication and identity proofing processes based on, in part, updated definitions of "authentication" and "authorization," and the introduction of the idea of "identity proofing."

4. Cybersecurity Measurement

Through the use of "measures" set forth in the Proposed Update, an organization can measure and demonstrate the effectiveness of its cybersecurity risk management procedures.

April 10, 2017 is the Cutoff for Public Comment on the Proposed Update

Businesses have until April 10, 2017 to submit comments to NIST before the Proposed Update goes into effect.

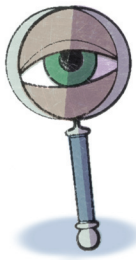
Additional Assistance

Because we know that many organizations look to NIST for cybersecurity guidance, Phillips Lytle's Data Security & Privacy Practice Team will continue to monitor the Proposed Update. Please contact Jennifer A. Beckage, F. Kenneth Graham or any member of the firm's Data Security & Privacy Practice Team if you have any questions about the Proposed Update, or how NIST or other guidance may apply to your business. We can also assist in policy drafting, from defensible record retention and destruction methods to crisis planning; data breach response, mitigation and notification; and evaluating an organization's transfer, storage and use of data. ■

PHILLIPS LYTLE LLP CLIENT ALERT

DATA SECURITY & PRIVACY

FEBRUARY 2017



Data Security & Privacy Team

Jennifer A. Beckage (716) 847-7093, (212) 759-4888 ext. 7093, (585) 238-2000 ext. 7093 jbeckage@phillipslytle.com
Edward S. Bloomberg (716) 847-7096, (212) 759-4888 ext. 7096 ebloomberg@phillipslytle.com
Alan J. Bozer (716) 504-5700, (212) 759-4888 ext. 5700 abozer@phillipslytle.com
Mary E. Burgess (518) 472-1224 ext. 1231 mburgess@phillipslytle.com
Anna Mercado Clark (212) 508-0466 aclark@phillipslytle.com
Jeffrey D. Coren (716) 847-7024 jcoren@phillipslytle.com
John M. Falk (202) 617-2723 jfalk@phillipslytle.com
Chad W. Flansburg (585) 238-2009 cflansburg@phillipslytle.com
F. Kenneth Graham (716) 847-7049 fkgraham@phillipslytle.com
Asaf Hahami (212) 508-0432 ahahami@phillipslytle.com
Patrick M. Hanley, Jr. (716) 847- 8306 phanleyjr@phillipslytle.com
Richard E. Honen (518) 472-1224 ext. 1225 rhonen@phillipslytle.com
Luke B. Kalamas (585) 238-2035 lkalamas@phillipslytle.com
Timothy P. Kucinski (716) 847-7056 tkucinski@phillipslytle.com
Brendan S. Lillis (716) 847-7058 blillis@phillipslytle.com
Richard J. Marinaccio (716) 504-5760 rmarinaccio@phillipslytle.com
Mark J. Moretti (585) 238-2004, (212) 508-0404 mmoretti@phillipslytle.com
William V. Rossi (716) 847-7022 wrossi@phillipslytle.com
John G. Schmidt Jr. (716) 847-7095, (212) 508-0426 jschmidt@phillipslytle.com
James Kevin Wholey (202) 617-2714 jwholey@phillipslytle.com

Phillips Lytle LLP

Albany Omni Plaza 30 South Pearl Street Albany, NY 12207-3425 (518) 472-1224
Buffalo One Canalside 125 Main Street Buffalo, NY 14203-2887 (716) 847-8400
Chautauqua 201 West Third Street Suite 205 Jamestown, NY 14701-4907 (716) 664-3906
Garden City 1205 Franklin Avenue Plaza Suite 390 Garden City, NY 11530-1629 (516) 742-5201
New York City 340 Madison Ave 17th Floor New York, NY 10173-1922 (212) 759-4888
Rochester 28 East Main Street Suite 1400 Rochester, NY 14614-1935 (585) 238-2000
Washington, DC 800 17th Street NW Suite 450 Washington, DC 20006-3962 (202) 617-2700
Canada The Communitech Hub 151 Charles Street West Suite 152 The Tannery Kitchener, Ontario N2G 1H6 Canada (519) 570-4800