Client Update
New Federal Guidance on Cybersecurity for Mobile Devices

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Jonathan Metallo
jmetallo@debevoise.com

On November 4, the National Institute of Standards and Technology ("NIST"), an arm of the Department of Commerce, issued a new draft practice guide entitled "Mobile Device Security: Cloud & Hybrid Builds." This represents NIST's growing focus on mobile security – a subject NIST has touched on before, but did not specifically address in its much-ballyhooed 2014 "Framework for Improving Critical Infrastructure Cybersecurity," better known as simply the Framework. NIST has opened its Mobile Device Security practice guide to public comment until January 8, 2016.

The Mobile Device Security guidance was issued by NIST's National Cybersecurity Center of Excellence ("NCCoE"), a partnership among NIST and companies in the technology industry. The guidance emerged from NIST's collaboration with Microsoft, Intel, Lookout and Symantec.

NIST has established itself as a standard-bearer in cybersecurity benchmarking. The 2014 NIST Framework, although designed on its face for use by "critical infrastructure" organizations, has been widely adopted across the private sector. NIST's leadership impact has been felt not only from a technical and business perspective but from a legal one as well.

For example, Commissioner Julie Brill of the U.S. Federal Trade Commission – an agency that brings many cases against companies over their allegedly inadequate cybersecurity – has lauded the 2014 NIST Framework as "fully consistent with the FTC's enforcement framework." The U.S. Securities and Exchange Commission has encouraged funds and investment advisers to "consult this Framework when considering a strategy to mitigate exposure to cyber attacks." The U.S. Department of Justice likewise has cited the NIST Framework as a key source for cybersecurity guidance.

Leading accounting firms and insurance companies, too, have taken note of the NIST Framework. At least one major insurer has started to incorporate the Framework into its underwriting for cyber coverage.

Companies looking to stay ahead of the regulatory and market curve on cybersecurity might therefore do well to consider NIST's new draft recommendations. The reasons for concern about mobile security in the corporate context are clear. Bring Your Own Device ("BYOD") programs, for example, are widely recognized as a threat vector; in the BYOD environment, companies lack control over what employees may download to their personally owned devices when not connected to the company network. One popular alternative to BYOD is the so-called Corporate Owned and Personally Enabled device, or COPE – where the company provides a smartphone or tablet to an employee, who is free to customize it and to use it for both business and personal purposes. COPE is generally considered less risky than BYOD, but still presents the risks of commingling the employee's personal uses and data with the company's.

NIST's new draft guidance maps out in some detail how companies might mitigate the security risks caused by employee use of mobile devices. This makes it quite different from the NIST Framework, which speaks more in terms of broad categories of issues and tends to leave implementation details to a company's discretion. The mobile security draft includes a 144-page "How-To" guide that covers topics such as:

- configuring mobile devices, *e.g.*, by implementing an entirely cloud-based or hybrid solution;
- separating the company's data and employee personal data stored on or accessed from the mobile device, *e.g.*, by leveraging Operating System capabilities to prevent user-level applications from exchanging data with each other, thereby "sandboxing" sensitive applications; and
- de-provisioning mobile devices that no longer require access to company data (lost devices, stolen devices, devices of employees leaving the company), *e.g.*, by configuring devices to automatically wipe all stored data after a certain number of failed authentication attempts.

The new draft guidance goes so far as to cite specific, commercially available products (Microsoft Office 365, Lookout's Android application for detecting malicious software, and Symantec's Secure Site Pro service for generating digital authentication certificates) that might be used to help configure a mobile device

management system. NIST specifically notes it is not endorsing the products named in the practice guide.

We have compared notes on the new NIST guidance with our colleagues at Stroz Friedberg, a leading cybersecurity firm. Edward Stroz, the firm's Executive Chairman, observes:

"The impact of mobile devices in enterprise security is often underestimated, in part because legacy best practices for enterprise security lag developments in mobile technology. In most enterprise environments today, the number of mobile devices often equals or surpasses the number of desktops and laptops. The NIST document recognizes that the widespread adoption of mobile devices to communicate, search, and access sensitive information poses a potential threat to information security measures because traditional boundaries established between trusted and untrusted systems are vanishing.

"As mobile devices are used to store sensitive enterprise data and pose a higher risk of loss or theft, needed controls must be prioritized to prevent or mitigate potential information loss. In this context, we expect that the NIST Cybersecurity Practice Guide on Mobile Device Security will be helpful to companies by providing scientific, prioritized guidance following a risk-based methodology, in much the same way as the NIST Cybersecurity Framework has."

What actions might organizations want to consider taking right now in light of the new draft guidance from NIST?

- Given the impact of the existing NIST Framework on both technical and legal standards, it is not too soon for legal departments to consult with their colleagues in IT, IT security, risk and other key stakeholders and begin assessing how the organization's mobile security practices stack up against the new draft guidance. Nor is it too soon to begin planning and implementing any remedial steps that might be appropriate in light of the guidance.
- Organizations that wish to be heard on the substance of the draft guidance have the option of submitting comments to NIST. The comment period runs until January 8, 2016, a relatively tight timeline given the holiday season.

* * *

Please do not hesitate to contact us with any questions.