wiley

NEWSLETTER

Cybersecurity Developments: Does the NIST "Voluntary" Framework Portend New Requirements for Contractors?

Fall 2013

Cybersecurity promptly reemerged as a hot topic for the federal acquisition community shortly after the Government reopened from the shutdown. On October 22, the National Institute of Standards and Technology (NIST) released a much-anticipated preliminary "framework" of standards and practices designed to assist critical infrastructure organizations addressing and managing cybersecurity risk. The same day, DOD issued a final rule expanding the Defense Industrial Base (DIB) Voluntary Disclosure Program, finalizing an interim rule issued in May. Both steps reflect further progress in implementing President Obama's Executive Order (EO) 13636, but questions still remain eight months after the EO as to the ultimate content and structure of the NIST framework and the impact both programs will have on government contractors. Chief among those questions for government contractors is whether, and how, the programs could eventually sprout new minimum requirements for companies doing business with the federal Government. On November 18, DOD moved forward with a final rule imposing new basic security requirements for certain types of technical data and mandatory disclosure obligations for certain cyber incidents and breaches.

NIST's Preliminary Cybersecurity Framework. The preliminary framework represents months of collaboration between NIST, Government, and industry stakeholders to identify and characterize cybersecurity best practices. EO 13636 instructed NIST to develop "a prioritized, flexible, repeatable, performance-based and cost-effective approach" to "align policy, business, and technological approaches

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

to address cyber risks." Over the past six months, NIST has engaged industry participants through a series of national workshops to gather input on existing industry standards, guidance and best practices to achieve outcomes that can assist organizations in managing their cybersecurity risk. The voluntary framework is designed to enhance critical infrastructure organizations' existing business or cybersecurity risk management processes and cybersecurity programs by identifying potential gaps and filling them with standardized best practices. Comments on the preliminary framework are due in early December, and a final framework is anticipated in February 2014.

The framework is intended to complement existing business and cybersecurity operations for organizations with formal existing plans and policies, or to serve as a template for organizations that create new programs. It features a series of four progressive "Implementation Tiers" to describe how an organization manages cybersecurity risk. This risk-based assessment "describe[s] an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is integrated into an organization's overall risk management practices." Framework participants will use the four-tier structure to characterize the organization's existing risk management profile and compare it with the tier that best aligns to the organization's cyber risk profile. The expectation is that framework participants will align the organization's profile to the best practices established for each successive tier.

The NIST framework is intended to be a voluntary program. Industry has insisted, however, that voluntary participation should be encouraged through a series of incentives, which remain very much in the ether. In August, a post to the White House blog by the President's Cybersecurity Coordinator highlighted areas in which potential incentives were being analyzed and discussed by "the Administration, Congress, and private sector stakeholders." Those areas include (1) cybersecurity insurance; (2) grants; (3) process preferences (primarily for technical assistance in responding to cyber incidents); (4) legislation to limit liability for cyber incidents for framework participants; (5) streamlined regulatory structures and reduced audit burdens; (6) public recognition; (7) rate recovery for price-regulated industries; and (8) Government assistance with cyber-related research initiatives.

For government contractors, in particular, one "incentive" agencies could adopt—either through formal rulemaking or on an ad hoc basis—is a preference for framework participants in competitions for federal information technology (IT) or cyber-related contracts. Contractors are also wary that the voluntary NIST framework could be a prelude to new "mandatory" cybersecurity requirements for federal acquisitions, either through contract-specific standards of care requirements or through formal rulemaking. Much as the FAR Councils required contractors to implement standards of business ethics and conduct (FAR 52.203-13) in 2008, the NIST framework could serve as the template for new cyber requirements. The new DOD final rule on Safeguarding Unclassified Controlled Technical Information (discussed below) appears to be a first step in that direction.

Some industry participants have also expressed concern that the NIST framework will lead to a *de facto* baseline for all industry participants if it is recognized as the new industry standard of care. In that case, they argue, any cyber program that falls short of the NIST framework could expose an organization to liability for not following established best practices. In this respect, the "voluntary" NIST framework would exert a

gravitational pull that would force industry participants to align their practices—either to obtain the benefits of Government "incentives" or to avoid the risk of having a cyber program that no longer measures up to the new standard.

Final DIB Voluntary Disclosure Rule. DOD finalized its interim rule on the DIB voluntary disclosure program. *See* 78 Fed. Reg. 62431 (Oct. 22, 2013). The final rule reflects DOD's effort to continue to grow the program to include more DIB participants and increase the Government and DIB situational awareness of the extent and severity of cyber threats to DOD information residing on DIB networks. The program has grown to more than 100 participants, and is part of DOD's approach to enhance and supplement DIB information assurance and threat awareness capabilities. We previously covered DOD's interim rule in May 2012, and the final rule leaves the interim rule largely unchanged, although DOD did clarify the scope of "U.S.-based" systems on which participants may deploy countermeasures based on government-furnished information received under the program. The final rule also deleted a statement that DOD "may request from any DIB participant additional information or assurances" from the DIB participant regarding the organization's cyber policies or practices, based on industry concerns that this could implicate attorney-client privileges. DOD clarified in its preamble comments, however, that it retained the authority to request additional information from participants.

Final DOD rule on Safeguarding Unclassified Controlled Technical Information. DOD also finalized a proposed rule on safeguarding certain types of controlled technical information that is stored on or transits across contractors' unclassified information systems. *See* 78 Fed. Reg. 69273 (Nov. 18, 2013). The new final rule reduces the scope of an earlier proposed rule that would have imposed data security requirements on a broad range of unclassified DOD information, and restricts the rule to "unclassified controlled technical information," which includes all technical data and computer software (as defined in DFARS 252.227-7013) with military or space application that is subject to DOD access controls. This includes, for example, research and engineering data, engineering drawings, specifications, manuals, technical reports, and computer software. The final rule requires affected contractors to "provide adequate security to safeguard unclassified controlled technical information from compromise." The minimum standards to be applied to affected unclassified information technology systems are drawn from fairly standard commercial practices outlined in NIST Special Publication (SP) 800-53 to control and protect affected systems. The NIST SP 800-53 standards are already fairly ubiquitous in DOD contracts, and DOD anticipates that the new requirements will therefore come at little additional cost to the industry, overall. At a minimum, contractors must implement access controls, awareness and training, contingency planning, identification and authentication, and maintenance.

The potentially more onerous and significant obligation imposed by the new rule is a mandatory reporting requirement where unclassified, controlled technical information residing on or transiting through a contractor's unclassified system is potentially exfiltrated, manipulated, or otherwise lost or compromised. Contractors must also report any incidents resulting in unauthorized access to their covered systems. These triggering events are subject to some ambiguity, and contractors will need to give careful consideration to whether a cyber incident triggers the reporting obligation. If so, the new reporting obligation requires contractors to report cyber incidents to DOD within 72 hours of discovering the incident. Incident reports will

trigger significant additional obligations for the contractor to assess its networks and capture information related to the reported incident, and potentially support DOD damage assessments.

DOD's initial proposed rule had included additional "basic" security requirements for a broader range of unclassified nonpublic information. That aspect of the rule was subsequently overtaken by a proposed FAR rule, FAR case 2011-020, Basic Safeguarding of Contractor Information Systems, that would impose similar safeguarding requirements on all federal contractors. In its preamble comments on the final rule, DOD indicated that a final FAR rule would be forthcoming to address those "basic" safeguarding requirements. As a practical matter, many DOD contractors are already subject to these "basic" safeguarding requirements, which have been incorporated into many DOD contracts by reference to DOD Instruction 8582.01, Security of Unclassified DOD Information on Non-DOD Information Systems (June 6, 2012).