Bloomberg BNA

Privacy and Security Law Report®

Reproduced with permission from Privacy & Security Law Report, 14 PVLR 1010, 06/08/2015. Copyright © 2015 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Threats to the Supply Chain: Extending Federal Cybersecurity Safeguards to the Commercial Sector

BY ROBERT S. METZGER

Government and private sector functions depend substantially upon information and communication technology.[1] President Barack Obama's 2016 budget proposes spending $86.4 billion on federal information technology—the majority of which, $49.1 billion (57 percent), is for nondefense functions.[2]

Cyber threats are posed to information and communications technology (ICT) systems operated by the federal government and by its contractors. Federal interests are in jeopardy if sensitive government data, residing in or transiting through such systems, are destroyed, compromised or stolen. Consequences include impairment of government and private sector functions and loss, corruption or improper use of sensitive and proprietary data.

A Vulnerable Supply Chain

The ICT supply chain is a:

> complex, globally distributed, and interconnected ecosystem that is long, has geographically diverse routes, and consists of multiple tiers of outsourcing. This ecosystem is composed of public and private sector entities (e.g., acquirers, system integrators, suppliers, and external service providers) and technology, law, policy, procedures, and practices that interact to design, manufacture, distribute, deploy, and use ICT products and services.[3]

Federal agencies have adopted and regularly employ this ecosystem, which increases their reliance upon commercial sources and service providers.

The security of federal information often depends upon measures taken by its contractors (and their suppliers). That the federal government in 2011 adopted a ''cloud first'' policy further divests federal agencies of direct authority over systems that host, transmit or employ federal information.[4]

The ICT supply chain has many points of vulnerability. While the threats differ and the attack vectors are diverse, vulnerability is present at levels that extend to individual electrical, electronic or electromechanical parts as well as electronic assemblies, systems and networks. Areas that may be vulnerable to hostile cyber acts include hardware, where electronic parts exercise control functions, as well as firmware and software.

The global nature of the information technology supply chain contributes to the proliferation of these risks. Because of omnipresent interconnection, and increasing use of information services that depend upon externally managed services, cloud infrastructure and Web-enabled delivery, threats to information systems may be

[1] The U.S. Census Bureau reports that, in 2011, U.S. nonfarm businesses with employees spent a total of $289.9 billion on noncapitalized and capitalized information and communications technology (ICT) equipment, including computer software. Information and Communication Technology Survey, U.S. Dept. of Commerce, *available at* http://www.census.gov/econ/ict/.

[2] President's Budget for Fiscal Year 2016, ch. 17, p. 281, *available at* http://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/ap_17_it.pdf.

Rogers Joseph O'Donnell PC is a boutique law firm that has specialized in public contracts for more than 33 years.

Robert S. Metzger is a shareholder and heads the firm's Washington office. This article presents his individual views and shouldn't be attributed to any client of Rogers Joseph O'Donnell or to any organization with which Metzger is or may be affiliated.

[3] National Institute of Standards & Technology (NIST) Special Publication (SP) 800-161 (''Supply Chain Risk Management Practices for Federal Information Systems and Organizations'') (4/15/15), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[4] *See* ''Security Authorization of Information Systems in Cloud Computing Environments,'' Memorandum for Chief Information Officers, 12/8/11, *available at* https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf.

COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 1538-3423

directed at the ''weakest links'' of connected enterprises.

Federal agencies employ a variety of controls to protect sensitive information when it is within the domain or authorization boundary of ''federal information systems.'' But vast amounts of federal information are constantly in the hands of the external federal supply chain. As to this wealth of information, in commercial systems, the presence of security controls is problematic at best.

With limited exceptions,[5] no statute or regulation generally imposes any contractual obligation upon federal commercial contractors to protect against cyber threats, inclusive of *physical* threats, such as posed by counterfeit electronic parts; *cyber-physical* threats, as represented by maliciously encoded (''tainted'') electronic parts; and *cyber*threats as are posed to ICT systems through network interconnection. As explored in my previous articles,[6] the Department of Defense (DoD) has taken initiatives, using its acquisition authority, to address its supply chain risk in all three areas.[7]

Corresponding action has not yet been taken on the civil side of federal contracting. Yet, the commercial supply chain that supports federal civil functions is exposed to substantially the same or similar risks. Federal agencies apply a variety of cybersecurity controls to contractors who operate ICT as ''federal information systems.''[8] While distinct, ''nonfederal information systems'' also are within the zone of important government interests. These are systems operated by companies or other organizations that are entrusted with, use or transmit sensitive nondefense federal information. There are many categories of such information, which collectively constitute federal ''controlled unclassified information'' (CUI).[9] CUI encompasses many types of federal information in diverse categories.[10] CUI stored, used or communicated through private (nonfederal) ICT systems must be protected against cyber threats. Absent any legislative mandate, federal civil agencies can and should use their *acquisition authority* to protect this information. In so doing, federal contracting authority will cause broad segments of industry that supply to and support the federal government to improve cybersecurity and supply chain risk management practices.

Protecting CUI—Crucial Questions

The National Institute of Standards and Technology (NIST) is working now to complete Special Publication (SP) 800-171, a control regime to protect CUI on nonfederal information systems.[11] Before this can be applied to federal contractors, however, several crucial questions must be resolved that are outside NIST's authority.

The first is definitional. For years, the federal government has struggled to reconcile conflicting definitions of CUI.[12] Security controls to protect CUI will not be successful if neither agencies nor companies know what information is CUI. The National Archives and Records Administration (NARA) has the responsibility to promulgate the regulations needed to resolve this uncertainty. On May 8, NARA issued a proposed rule to add a new Part 2002 (''Controlled Unclassified Information (CUI)'') as a new Part 2002 of Title 32 of the Code

---

[5] Certain restrictions are imposed, however, by Section 515 of the FY 2014 Omnibus Appropriations Act and made applicable to the Departments of Commerce and Justice, the National Aeronautics and Space Administration and the National Science Foundation. The same language is also present in Section 515 of the FY 2015 consolidated appropriations measure that funds these agencies. Funds appropriated for these agencies may not be used to acquire a ''high-impact'' or ''moderate-impact'' information system unless the agency has (1) reviewed the supply chain risk against criteria developed by the NIST; (2) reviewed the supply chain risk from the prospective awardee against available threat information; and (3) conducted an assessment of the risk of cyber espionage or sabotage associated with the acquisition of such system. In addition, none of the funds appropriated for these agencies may be used to acquire a ''high-impact'' or ''moderate-impact'' information system unless a mitigation strategy has been developed in coordination with NIST, a determination has been made that the acquisition is in the national interest and a report has been made to the Congressional appropriations committees.

[6] *See* Robert S. Metzger & Lucas T. Hanback, *DOD's Cybersecurity Initiative—What the Unclassified Controlled Technical Information Rule Informs Public Contractors About the New Minimums in Today's Cyber-Contested Environment*, 102 Bloomberg BNA Fed. Cont. Rep. 744 (12/30/14) (14 PVLR 60, 1/12/15); Robert S. Metzger, *Convergence of Counterfeit and Cyber Threats: Understanding New Rules on Supply Chain Risk*, 101 Bloomberg BNA Fed. Cont. Rep. 164 (2/18/14).

[7] DoD policy is to manage ''the risk that a foreign intelligence or other hostile elements could exploit supply chain vulnerabilities to sabotage or subvert mission-critical functions, system designs, or critical components.'' Dep't of Defense, ''Assured Microelectronics Policy,'' (July 2014), *available at* http://www.acq.osd.mil/se/docs/DoD-Assured-Microelectronics-Policy-RTC-July2014.pdf.

[8] A ''federal information system'' is defined as an information system used or operated by an executive agency, by a contractor of an executive agency or by another organization on behalf of an executive agency. 40 U.S.C. § 11331; *see also* Federal Information Processing Standards Publication (FIPS) 200 (''Minimum Security Requirements for Federal Information and Information Systems'') (Mar. 2006), at app. A, p.7.

[9] Executive Order 13556 of Nov. 4, 2010, ''Controlled Unclassified Information,'' *available at* http://tinyurl.com/n4rnqkj (9 PVLR 1592, 11/22/10). The executive order states as its purpose to ''establish a uniform program for managing information that requires safeguarding or dissemination controls.'' The National Archives and Records Administration (NARA) is the executive agent assigned to implement E.O. 13556.

[10] The NARA website presents information about ''CUI Categories and Subcategories,'' *available at* http://www.archives.gov/cui/registry/category-list.html#categories. The CUI Registry maintained by NARA, while a work-in-progress, enumerates many categories and subcategories of information that reside regularly on ''nonfederal information systems'' as well as ''external information systems.'' (These are defined in n.11, *infra*.)

[11] A ''nonfederal information system'' is defined as ''[a]n information system that does not meet the criteria for a federal information system.'' NIST SP 800-171(''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations'') (Final Public Draft) (April 2015), *available at* http://csrc.nist.gov/publications/drafts/800-171/sp800_171_second_draft.pdf (14 PVLR 657, 4/13/15).

[12] NARA has noted that ''[t]here are currently over 100 different ways of characterizing [sensitive but unclassified] information,'' and that ''there is no common definition, and no common protocols describing under what circumstances a document should be marked . . . and what procedures should be followed for properly safeguarding or disseminating [sensitive but unclassified] information.'' NARA FAQs at 2, *available at* http://www.archives.gov/cui/faqs.html.

 COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

of Federal Regulations.[13] The rule uses the ''CUI Registry'' to identify 23 discrete categories and 82 subcategories of CUI.

NARA seeks to control the designation of CUI. Its proposed rule asserts that agencies ''may not control any unclassified information outside of the CUI program.'' NARA would allow agencies to designate CUI only if approved by NARA as the CUI Executive Agent.[14] While the CUI rule is not final, one can anticipate tension between the ''gatekeeper'' role that NARA intends to play and the likelihood that federal agencies will assert authority over which of their information should be designated as CUI.

A related question is how agencies and their suppliers will be informed that information has been categorized as CUI. The proposed NARA rule asserts that agencies ''must mark CUI'' according to ''marking guidance'' that NARA will issue.[15] NARA's proposed rule also insists that agencies may not use any marking or designation practices other than as established by NARA in the rule and the CUI Registry.[16] The proposed rule is to be commended for its effort to establish common definitions to categorize CUI, for its assignment of designation responsibilities to agencies and for its emphasis upon uniform marking practices. How well these practices extend to information that is communicated or stored electronically, however, remains to be seen. Contractors will be concerned that the proposed rule could leave them liable for failure to apply required safeguards even if the government agency that supplied the information to them failed to mark it as CUI. The proposed rule states that the ''lack of CUI marking does not exempt the information from applicable handling requirements set forth in laws, regulations or Government-wide policies.''[17] The proposed rule does not address the situation where a government contract requires a company to create a product or to provide a result that will constitute CUI under the approved CUI Registry definitions.[18]

A further and crucial question is what level of safeguarding will be applied for CUI or the various categories and subcategories articulated in the CUI Registry. NARA's proposed rule sets a ''*Basic*'' safeguarding standard, which it describes as ''the default set of standards agencies must apply to all CUI'' unless the CUI Registry specifies otherwise.[19] CUI may be subject to a different and potentially higher standard, ''*CUI Specified*,'' only when explicitly provided in the CUI Registry.[20] In its proposed rule, NARA reserves for itself, as CUI Executive Agent, exclusive authority both to issue and to update the safeguarding standards in the CUI Registry.[21] An anchor tenet of the proposed rule is that the categorization, safeguarding and dissemination controls of CUI are determined strictly in accordance with ''laws, regulations, or Government-wide policies.'' The *CUI Specified* safeguarding standards apply only to CUI categories and subcategories ''that have specific handling standards required or permitted by authorizing laws, regulations, or Government-wide policies.''[22] Absent such authorization (and NARA's approval), it seems that agencies cannot elevate or diminish safeguards from what NARA dictates as *CUI Basic*. The proposed rule asserts that agencies ''may not require anyone outside the agency [e.g., contractors] to use a higher impact level or adopt more stringent security requirements and controls'' than NARA determines to be appropriate for internal practices of the agency.[23] As for the safeguards themselves, NARA's proposed CUI defers to NIST and SP 800-171 for the cybersecurity safeguards to be required of commercial companies that host, use or transmit CUI. In the promulgation comments accompanying the proposed rule, NARA states that it has ''partnered with NIST'' to develop information system security requirements for ''the contractor environment'' with the intent of making it ''easier for businesses to comply with the standards using the systems they already have in place.''[24]

Industry may welcome the objective of standardization of safeguards for federal agencies to insist upon when it comes to handling their CUI. Whether this will come to be as NARA proposes is dubious. Agencies are in the best position to identify information in their domain that merits protection against cyber threats. They may be in the best position to know where vulnerabilities exist in external (contractor) information systems that expose their CUI to cyberattack. Agencies also are best able to assess the impact to their operations should the confidentiality (or integrity) of their CUI suffer compromise. All these considerations suggest that agencies will insist upon greater authority over the level of safeguards to be applied to companies that possess the agencies' CUI. While the NARA rule provides for a special and potentially more demanding level of controls for *CUI Specified*, today the CUI Registry does not specify what those controls are or might be, and there is reason to doubt that agencies will acquiesce to having NARA decide in all cases on whether more controls or needed or what those controls will be. At the same time, agencies also should be aware that elevating controls beyond the *CUI Basic* norm can produce potentially dysfunctional consequences. Some capable and trustworthy commercial suppliers will refuse to adopt special and more demanding controls. Some companies may exit the federal marketplace altogether if they cannot reconcile special federal cyber control obligations with their general enterprise systems, or if the costs cannot be recovered. Isolated, contract-specific or CUI category-specific controls that increase contractor costs will mean higher costs to agencies that demand them. For all these reasons, and more, each federal agency should weigh carefully whether to impose cyber control requirements beyond what NARA envisions and what NIST will recommend in SP 800-171. Still, at this junc-

[13] 80 Fed. Reg. 26,501 (May 8, 2015). Comments on the proposed rule are due on or before July 7, 2015.

[14] Proposed 32 C.F.R. § 2002.11 (a), (b), 80 Fed. Reg. 26,506.

[15] *Id.* at § 2002.13(a)(3), 80 Fed. Reg. 26,507.

[16] *Id.* at § 2002.15(a), 80 Fed. Reg. 26,508.

[17] *Id.* at § 2002.15(a)(8), 80 Fed. Reg. 26,508.

[18] This can be dealt with contractually, however. For example, the final NARA CUI rule could instruct federal agencies to incorporate the necessary designation and marking instructions in contractual documentation such as the Data Item Description (DID), Contract Data List Requirements List (CDRL), in the Statement of Work or otherwise.

[19] *Id.* at § 2002.12(b)(1), 80 Fed. Reg. 26,506.

[20] *Id.* at § 2002.12(b)(2).

[21] *Id.* at § 2002.12(a)(4).

[22] *Id.* at § 2002.2, 80 Fed. Reg. 26,504.

[23] *Id.* at § 2002.12(g)(2), 80 Fed. Reg. 26,507.

[24] 80 Fed. Reg. 26,503.

ture, neither agency nor industry can foresee whether the federal CUI cybersecurity initiative will produce a generally applicable set of commercially acceptable cybersecurity safeguards, with limited exceptions, or a patchwork of specialized and different demands that industry will find very burdensome.[25]

Boundary-Setting Problems

Tough questions are present as the federal government seeks to define and designate CUI and to establish a mechanism to require its safeguarding that is at once workable in commercial contractor environments and sufficient to respect bona fide agency concerns. A further analytic problem is present in the pervasive difficulty, in an interconnected world, of setting control boundaries for ''federal information systems'' as distinct from ''nonfederal'' or ''external'' information systems.[26] In SP 800-171, NIST articulates security controls for ''nonfederal information systems'' that reflect but are tailored downward from comparable controls that the federal government imposed upon systems within its own ''authorization boundary'' to protect similar or identical information. This likely reflects NIST's recognition of adverse cost/benefit consequences and practical implementation challenges should the whole of the NIST control architecture be pushed out to the thousands and thousands of companies in the federal supply chain. This broader context—fitting NIST's federally-derived systems into markets where the federal role may be only incidental—poses its own challenges.

SP 800-171 evidences effort by NIST to reconcile its controls with other regimes and methods already employed in the private sector. The importance of the proposition is difficult to overstate. Federal agencies ultimately will pay the costs of mandatory cybersecurity measures imposed upon the federal supply chain. Those costs may be higher prices for supplies or services or lost access to sources that choose not to accommodate the federal demands. Means must be found to achieve the objectives of NARA and NIST to better safeguard CUI without denying or superseding the validity of other strategies and techniques as may be sufficient, but different.

[25] The proposed CUI rule appears to make many compromises in the pursuit of uniformity and predictability. One is in its decision to categorize all CUI as at the ''moderate confidentiality impact level'' of FIPS 199. Proposed 32 C.F.R. at § 2002.12(g)(2), 80 Fed. Reg. 26,507. Agencies may conclude that particular categories or subcategories of their information have less impact, or more, with corresponding implications for both controls and oversight. Similarly, the present draft of SP 800-171 seeks to protect just the ''confidentiality'' of information in nonfederal systems, but not ''integrity'' or ''availability.'' SP 800-171 (Final Public Draft), at 2. If agencies see risk to their mission should a commercial ICT system become unavailable due to cyberattack, they may insist upon upward tailoring of applicable CUI cybersecurity requirements.

[26] NIST comments: ''[F]ederal information designated as CUI has the same intrinsic value and potential adverse impact if compromised—whether such information resides in a federal or a nonfederal organization. Thus, protecting the confidentiality of CUI is critical to the mission and business success of federal agencies and the economic and national security interests of the nation.'' SP 800-171 (Final Public Draft), at 5.

Cyber Threats to Federal Information—and Citizen Privacy

Cyber threats are very much in the public mind. Most of the publicized attacks have been against the private sector. The hack of Sony Pictures Entertainment Inc. brought down that company's information systems and disrupted day-to-day operations, while the release of supposedly ''private'' information caused great embarrassment. The attack on Anthem Inc. apparently compromised the health-care information of millions of insured persons. A recently reported cyber theft suggests that hundreds of millions of dollars were stolen from as many as 100 banks (or more) in the U.S., European Union and Russia. Those attacks warn that similar vulnerabilities are present in commercial ICT systems that host or act on federal information—with comparable (or worse) adverse consequences. Civilian federal agencies are responsible for CUI equal to or more sensitive than that taken from Anthem. They preside over funds even larger and financial functions even more important than those exposed by the bank cyber theft.

That CUI includes information that implicates important confidentiality interests of both individuals and our government is well stated in NIST SP 800-171:

> Many federal contractors, for example, routinely process, store, and transmit sensitive federal information in their information systems to support the delivery of essential products and services to federal agencies (e.g., providing credit card and other financial services; providing Web and electronic mail services; conducting background investigations for security clearances; processing health care data; providing cloud services; and developing communications, satellite, and weapons systems). Additionally, federal information is frequently provided to or shared with entities such as State and local governments, colleges and universities, and independent research organizations.[27]

There is official recognition of the serious and growing threat to government systems. The Government Accountability Office (GAO) has just released a report to Congress with this very disturbing summary:

> [C]yber threats and incidents to systems supporting the federal government and national critical infrastructures are increasing. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, advanced persistent threats—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks. Further underscoring this risk are the increases in incidents that could threaten national security, public health, and safety, or lead to inappropriate access to and disclosure, modification, or destruction of sensitive information. Such incidents may be unintentional, such as a service disruption due to an equipment failure or a natural event, or intentional, where for example, a hacker attacks a computer network or system. Over the past 8 years, the number of information security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) has increased from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent.[28]

[27] *Id.* at 1.

[28] ''High-Risk Series: An Update,'' Report GAO-15-290 (2/11/15), *available at* http://www.gao.gov/products/GAO-15-290 (14 PVLR 290, 2/16/15).

 COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

This report confirms that the cyber threat extends to federal information systems[29] operated by and for the civilian agencies as well as the nonfederal information systems of federal contractors and other organizations that receive, transmit or utilize CUI.

Using Acquisition Planning and Contract Administration to Improve Contractor Cybersecurity

Several regimes are in place for cybersecurity and information assurance for *federal* information systems. These include the Federal Information Systems Management Act (FISMA),[30] the Federal Information Processing Standards (FIPS), Federal Risk and Authorization Management Program (FedRAMP),[31] Office of Management and Budget (OMB) Circular No. A-130,[32] and the work of NIST. Particularly notable is NIST SP 800-53 (''Security and Privacy Controls for Federal Information Systems and Organizations''), revision 4, which updates and categorizes standards and guidelines for federal cyber controls, excepting national security systems,[33] and the Cybersecurity Framework, Version 1.0 (''Framework''),[34] which articulates voluntary industry standards and best practices to help diverse organizations manage cybersecurity risks.

The practices, controls and standards that ostensibly apply to federal information systems, however, do not now regularly extend to *nonfederal information systems*. The boundaries between ''federal'' and ''nonfederal'' information systems are difficult to distinguish.[35] NIST controls and practices, excepting the voluntary Framework, apply to executive agencies. However valuable, NIST controls do not apply to private contractors except to the extent that they are voluntarily assumed, invoked *by agencies* in the acquisition process (as necessary qualifications, for example), as part of competitive selection (in evaluation criteria) or imposed by a specific contract clause. In this sense, *acquisition methods* represent a crucial link between the cyber and supply chain objectives of NIST and their realization in the conduct of federal suppliers. That link is not now in place.[36]

Through issuance of Executive Order 13636 (''Improving Critical Infrastructure Cybersecurity''), Obama has encouraged voluntary adoption of cybersecurity measures to protect critical infrastructure.[37] Companies responsible for critical infrastructure include many who operate nonfederal information systems. Section 8 of the executive order establishes a ''Voluntary Critical Infrastructure Cybersecurity Program,'' to be coordinated among multiple federal agencies. Section 8(e) directs an inter-agency effort to assess the ''feasibility, security benefits, and relative merits of incorporating security standards into *acquisition planning and contract administration*.''[38]

Federal Market Power

That the federal government is expected to spend $90 billion on information technology (IT) in FY 2016 suggests it has market power sufficient to steer its supply chain to improve cybersecurity measures. Similarly, the very large companies that often control or operate critical infrastructure also should have sufficient influence

[29] ''Information system'' is defined as a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. *See* NIST SP 800-53, rev. 4, at app. B, B-5. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems and environmental control systems. NIST SP 800-161 (Apr. 2015), Ch. 1, at p.1.

[30] The General Services Administration (GSA) explains that ''FISMA requires federal agencies to implement a mandatory set of processes and system controls designed to ensure the confidentiality, integrity, and availability of system-related information.'' The processes and systems controls in each federal agency must follow established FIPS, NIST standards and other legislative requirements pertaining to federal information systems, such as the Privacy Act of 1974. GSA 2012 Agency Financial Report, ''Federal Information Security Management Act,'' *available at* http://www.gsa.gov/portal/content/150159.

[31] FedRAMP, according to the GSA, is a ''government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.'' GSA website, *available at* http://www.gsa.gov/portal/category/102371; *see also* http://cloud.cio.gov/fedramp.

[32] Circular No. A-130 establishes the federal government's information management policy. One attribute of that policy is to ''[p]rotect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information.'' OMB Circular A-130, 8.a(g), *available at* http://www.whitehouse.gov/omb/circulars_a130.

[33] NIST SP 800-53, rev. 4, *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (12 PVLR 774, 5/6/13).

[34] ''Framework for Improving Critical Infrastructure Cybersecurity,'' v. 1.0 (2/12/14), *available at* http://www.nist.gov/cyberframework/ (13 PVLR 281, 2/17/14). The Framework, created through the collaboration between industry and the public sector, is to serve as a model for companies to employ across critical infrastructure sectors.

[35] As observed by NIST in 2010, ''[e]xternal information system services are services implemented outside the [federal] authorization boundaries established by the organization for its information systems. These external services may be used by, but are not part of, organizational information systems.'' NIST SP 800-37 (''Guide for Applying the Risk Management Framework to Federal Information Systems'') (Feb. 2010), app. I, at p. I-1, *available at* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf (9 PVLR 362, 3/8/10). Cloud information services are delivered through the use of ''external information systems.''

[36] In the absence of plenary statutory obligation or federal regulations of general application, the acquisition authority and contracting practices of federal agencies provide the means to influence, if not to direct, the cybersecurity practices of the federal supply chain. This has been recognized by NIST for some years. In February 2010, NIST observed that ''[s]ecurity requirements for external providers including the security controls for information systems processing, storing, or transmitting federal information are expressed in appropriate federal contracts or other formal agreements.'' *Id.* at I-1.

[37] Executive Order 13636 (Feb. 12, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (12 PVLR 257, 2/18/13). E.O. 13636 defines ''critical infrastructure'' as ''systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.'' *Id.* at sec. 2.

[38] *Id.* at sec. 8 (emphasis added).

over their supply chain to obtain improved cyber and supply chain protection.[39]

DoD, which controls the most discretionary spending of any federal agency, already is using its contracting power—''acquisition planning'' and ''contract administration'' measures—to improve supply chain risk management of the defense industrial base. Defense Federal Acquisition Regulation Supplement (DFARS) regulations on unclassified controlled technical information (UCTI) use acquisition methods (contract clauses and flow-down requirements) to impact all companies in the DoD supply chain.[40] The UCTI DFARS shows how ''acquisition planning and contract administration'' can be used: The contract clause at DFARS 252.204-7012 (''Safeguarding of Unclassified Controlled Technical Information'') is to be used ''in *all* solicitations and contracts, including solicitations and contracts using Federal Acquisition Regulation (FAR) Part 12 procedures for the acquisition of commercial items.''[41] Through the required solicitation provisions and contract clauses, these regulations impose on DoD contractors (and their suppliers) minimum, NIST-derived security controls and establish required reporting procedures for many companies.

Federal civilian agencies are working to follow suit. Shortly after issuance of Executive Order 13636, the Joint Working Group on Improving Cybersecurity and Resilience through Acquisition was formed by DoD and the General Services Administration (GSA). The final report of the Joint Working Group was released Jan. 23, 2014.[42] The first of its six key recommendations is to institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions.

Prudent companies should now anticipate that the federal government will use acquisition and contract tools to require commercial suppliers to improve their cybersecurity measures. Some may question whether such federal ''intervention'' is necessary. Market forces (and enterprise self-protection) already motivate many in the federal supply chain to improve cyber supply chain measures. No doubt, some supply chain participants will seek competitive advantage by being early adopters of more rigorous controls. However, several considerations suggest that the federal government will not trust market forces or let industry proceed at its own pace. These include the direct risk to federal interests should the confidentiality of sensitive federal information be lost by reason of cyber breaches. Recent events in the private sector vividly demonstrate the costly and lasting injury that is the consequence of a successful cyberattack, even upon supposedly well-protected systems engaged in sensitive areas of commerce. The combined efforts of NARA and NIST have as their common purpose protecting sensitive federal information (CUI) against attacks of the same or similar character.

NIST SP 800-171

NIST SP 800-171 was first released in draft, for comments, Nov. 18, 2013.[43] The Final Public Draft was released in April 2015, and the comment period closed May 12. The final version of SP 800-171 could be released by mid-June 2015. Its purpose, as noted, is to protect the *confidentiality* of sensitive federal information (namely, CUI) that resides on *nonfederal* information systems. For *federal* information systems, in contrast, FISMA defines *three* security objectives for information and information systems: confidentiality, integrity and availability.[44] SP 800-171 also departs from its FISMA legacy in that it makes no distinction among relative *impact* of a security breach upon an organization or individuals. In contrast, FIPS 199 categorizes information and information systems based on the ''potential impact'' should adverse cyber events occur. ''Low'' impact is assigned if the consequence has a ''limited adverse effect;'' ''moderate'' impact is present where there is ''serious adverse effect;'' and ''high'' impact is present if effects are ''severe or catastrophic.''[45]

Importantly, FIPS 199 makes the determination of security categorization also a function of the ''information type,'' distinguishing among such types as ''public information'' (nonsensitive) or ''investigative information'' (very sensitive), and then examining impact as to *each* of the *three* security objectives (confidentiality, integrity and availability).[46] NIST SP 800-171, in contrast, does not discriminate among ''information types'' in setting security objectives. Consistent with the approach taken in NARA's proposed CUI rule, SP 800-171 treats all CUI as though it has the same sensitivity, and

[39] Debate continues as to whether the federal government has sufficient market power to persuade or compel sources of commercial-off-the-shelf (COTS) equipment to adopt federally mandated cyber and supply chain protection measures. Similarly, leading private sector enterprises may question whether they can impose controls upon their global sources. It is impossible to resolve these doubts. Independent of federal inducement or compulsion, however, the self-interest of both users and providers of ICT militate in favor of improved cyber protection. Those responsible for the assertion of federal interests should recognize that industry participants may have strategies and practices to address cyber threats which differ from those articulated by NIST but serve the same purposes sufficiently. Finding a means to assure protection of necessary federal interests without imposing a prescriptive or intrusive regime is a great challenge.

[40] DFARS: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039), 78 Fed. Reg. 69,273 (11/18/13) (12 PVLR 1987, 11/25/13).

[41] DFARS 204.7303, at 79 Fed. Reg. 69,280.

[42] *Improving Cybersecurity and Resilience through Acquisition*, *available at* http://tinyurl.com/kfuau32 (13 PVLR 212, 2/3/14).

[43] SP 800-171, ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,'' (Initial Public Draft), *available at* http://csrc.nist.gov/publications/drafts/800-171/sp800_171_draft.pdf (14 PVLR 657, 4/13/15).

[44] 44 U.S.C. § 3541. *See also* FIPS 199 (''Standards for Security Categorization of Federal Information Systems''), Feb. 2004, at 2; NIST ''Summary of NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations,'' 2/19/14, *available at* http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf. NIST explains that the objectives of integrity and availability ''maintain a high priority'' for organizations that seek a comprehensive information security program. SP 800-171 (Final Public Draft), at vi. NIST also observes that there is a close relationship between confidentiality and integrity ''since many of the underlying security mechanisms at the information system level support both security objectives.''

[45] FIPS 199, at 2-3. For each impact level, FIPS 199 provides ''amplification'' to explain the nature of consequences as would inform the categorization decision.

[46] *Id.* at 3.

 COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

no CUI receives a different control outcome as a function of *impact* in the event of a breach.[47]

Three Assumptions

As presently proposed, SP 800-171 makes three express ''assumptions'' that explain, albeit briefly, certain ''departures'' from the principles that apply to CUI on federal information systems.[48] One is that statutory and regulatory requirements for the protection of CUI are ''consistent,'' whether the information resides in federal or nonfederal information systems. The second is that the safeguards to protect CUI are ''consistent'' in both federal and nonfederal information systems and organizations. The third is that the ''confidentiality impact value'' of CUI is no lower than ''moderate'' in accordance with FIPS 199. The construct of SP 800-171 is built on these assumptions.

The support for these assumptions is questionable. Even if the requirements for the protection of CUI are the same, in fact the safeguards that NIST proposes to protect CUI, as set forth in SP 800-171, differ between federal and nonfederal information systems. Federal information systems are subject to the controls and enhancements specified in SP 800-53. For CUI in private hands, NIST proposes requirements that echo the purposes of SP 800-53 but are avowedly more accommodating of different methods. The stated assumption of SP 800-171 that the ''impact'' value of CUI is no lower than ''moderate'' likely reflects NIST's practical recognition that contractors will object to obligations that would require different control methods to distinguish between ''low'' and ''moderate'' impact. At the same time, the assumption of common impact can be criticized as commoditizing the many variations of CUI (recognized in the NARA Registry) and homogenizing actual differentials in true impact.

The departures from the FIPS norms and separation from SP 800-53 control baselines are ''concessions'' that NIST has made to improve the prospects that commercial organizations (and other CUI holders, such as state and local governments and educational institutions) will accept an extension of federal controls outside their present domain of federal information systems. This is commendable restraint, but not without some ''losses in translation.'' For example, for federal information systems FIPS 199 and FIPS 200 work in combination. FIPS 199 distinguishes among three categories of security objectives—confidentiality, integrity and availability. It also calls for assessment of the impact of a ''breach'' event, again using three categories, in this case ''low,'' ''moderate'' and ''high.'' FIPS 200 describes seventeen families of security controls. The level of security controls that a federal organization selects is a function of the identified impact levels for each of the three categories of security objectives. SP 800-171, in contrast, treats all impacts as ''moderate'' and addresses directly the single security objective of confidentiality. There may be practical benefits to this simplification, but it tends to ''normalize'' impact and ''marginalize'' the security objectives of system integrity and availability.

SP 800-171 claims a ''well-defined'' structure that consists of ''a *basic* security requirements section'' and a ''*derived* security requirements section.''[49] The former are drawn from FIPS 200, while the latter are based on NIST SP 800-53 at the ''moderate'' baseline. FIPS 200 describes ''Specifications for Minimum Security Requirements'' that fit into seventeen (17) discrete areas.[50] Viewed as a whole, SP 800-171 translates the 17 discrete security areas of FIPS 200 into 14 ''Security Requirements Families,'' leaving out three control families.[51]

In FIPS 200, the ''Minimum Security Requirements'' are very high-level, brief statements of objective, e.g.:

> **Access Control (AC):** Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.[52]

For the same family, ''Access Control,'' SP 800-53, revision 4, states 25 separate controls and several dozen available enhancements, and these are described over 51 pages of the publication. For this ''AC'' family, a total of 35 controls and enhancements must be met for the SP 800-53 ''moderate'' baseline.

The requirements for the ''Access Control'' family in SP 800-171 are much closer to FIPS 200 than to SP 800-53. They demand much less and are expressed at a much higher level. They consist of just two ''Basic Security Requirements'' and 22 ''Derived Security Requirements;'' all of the Derived Security Requirements are stated in a *single sentence*, and the whole treatment of the ''AC'' family of requirements in SP 800-171 takes less than *one* page.

The ''Requirements'' section of SP 800-171 informs companies about the safeguarding objectives. As concerning ''Access Control,'' for example:

> **3.1 ACCESS CONTROL**
>
> *Basic Security Requirements*:
>
> 3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

[47] Opportunities for ''tailoring'' are available under SP 800-171 (Final Public Draft); however, that could allow managers of information systems to increase the level of controls applied if they perceive that additional protection is necessary. Once federal agencies come to implement 800-171 through contract requirements, they may impose upward tailoring based upon the agency perception of impact. As suggested earlier, there appear to be inconsistencies between agency tailoring as contemplated by 800-171 and the feature of the proposed CUI rule by which NARA may intend to exclude agencies from imposing more stringent security requirements without its approval.

[48] *Id.* at 5.

[49] NIST SP 800-171 (Final Public Draft), at 6.

[50] These are: (i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity. FIPS-200, at 2.

[51] The control families that are missing are Configuration Accreditation & Security Assistance, Contingency Planning and Planning. Presumably, these were removed on the assumption that private sector operators will be responsible to perform these functions without need for federal standards. NIST SP 800-53 contains available controls and enhancements for all 17 FIPS 200 families.

[52] *Id.*

3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements:

3.1.3 Control the flow of CUI in accordance with approved authorizations.

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

[and so forth][53]

As the label implies, the ''Derived Security Requirements'' are based on the security controls in NIST SP 800-53, starting from the ''moderate'' controls baseline, but reduced to a subset through ''tailoring'' and expressed as brief principles rather than instructions. This was purposely done in order to avoid controls that are uniquely federal, unrelated to protecting just the confidentiality of CUI, or that NIST expects are routinely satisfied by nonfederal organizations without specification.

SP 800-171 lists 109 discrete requirements allocated to the 14 families that are to apply to CUI in nonfederal information systems. These requirements are ''mapped'' to identify relationships in the SP 800-53 security controls. The 109 requirements in SP 800-171 reference 85 controls from SP 800-53. This is considerably less than either the ordinary ''moderate'' baseline or the voluntary Framework, or even the SP 800-53 ''low'' baseline. Requirements described in SP 800-171 map to more SP 800-53 controls than DoD presently applies in its counterpart rule to protect UCTI:

References to NIST SP 800-53 Controls [54]

SP 800-53 HIGH	170 controls
SP 800-53 MODERATE	159 controls
VOLUNTARY FRAMEWORK	124 controls
SP 800-53 LOW	115 controls
SP 800-171	85 controls
DoD UCTI DFARS RULE	51 controls

Comparison of the number of cited controls should be undertaken with care. The intent of SP 800-171 is not to require contractors to comply strictly with controls (or control enhancements) from SP 800-53 just because NIST has provided tables that ''map'' the relationship. The intent is for companies who become subject to SP 800-171 to comply with the narrative statements in the Basic Security Requirements and the Derived Security Requirements for each of the 14 families; references to relevant controls or control enhancements from SP 800-53 are for information only. To satisfy the requirements of the SP 800-171, adoption of the SP 800-53 controls is not mandatory—or even encouraged. The strategy of NIST SP 800-171, instead, is to state *performance* or *capability-based* requirements that elaborate upon core principles drawn from FIPS 200 but do *not* express the ''how to'' rules of SP 800-53.

Through its 2013 regulations on UCTI, DoD has acted to impose limited security controls on its contractors that have access to unclassified technical information with military or space application. DoD's UCTI regulations invoke 51 of the SP 800-53 cyber controls (61 if ''enhancements'' cited in the DFARS are counted).[55]NIST SP 800-171 will articulate the requirements that apply to protect all categories and subcategories of CUI from all federal agencies, including the DoD UCTI that presently is subject to DFARS regulation. Both UCTI and CUI similarly concern unclassified but sensitive federal information.[56] Because of the convergence of the UCTI and CUI regulatory regimes, DoD can be expected to revise its DFARS after NIST SP 800-171 becomes final, and the SP 800-171 families of requirements will displace SP 800-53 controls and enhancements now invoked in the DFARS.

Federal authorities are well aware of the need to examine carefully what constitutes a sufficient level of controls and will seek industry views on this subject. Further education is needed to be sure that the affected contractor universe understands that the SP 800-171 requirements relate to but are independent from the catalog of SP 800-53 controls and control enhancements. But the uncertainty or dimensions of special agency-dictated controls and upward tailoring will remain very much in the minds of industry.

Implications of NIST SP 800-171 for Industry

As the federal government moves to impose its version of cybersecurity rules on nonfederal information systems and service providers, private industry will raise many questions of need, relevance, suitability, efficiency, burden, cost and justification. While some companies in the federal supply chain undoubtedly lack appropriate or even rudimentary controls, many companies already will have measures in place and may be subject to different if not conflicting sources of obligation or oversight as to those measures. Achieving the positive purpose of protecting sensitive federal CUI in nondefense contractors must be affordable, accomplished without costs disproportionate to benefits, without wholesale exclusion of capable and trustworthy companies and without new barriers that separate federal agencies from technology innovation in the commercial marketplace.

In the pending version of SP 800-171, NIST in several important ways recognizes these concerns:

- The enumerated security requirements are tailored down significantly from the controls and enhancements of the SP 800-53 ''moderate'' baseline.
- NIST accepts that nonfederal organizations can implement a variety of potential security solutions,

[53] SP 800-171 (Final Public Draft), at 9.

[54] *See* ''National Vulnerability Database,'' *available at* https://web.nvd.nist.gov/view/800-53/Rev4/impact?impactName=LOW. There are various complexities present in how to ''count'' either requirements or controls as referenced in the various documents, so these figures are illustrative only.

[55] 78 Fed. Reg. 69,281.

[56] ''Controlled Technical Information'' (CTI), as defined in DFARS 252.204-7012, means ''technical information with military or space application'' that is subject to controls. ''Controlled Unclassified Information,'' as defined in proposed NIST 800-171, app. B, at B-2, is ''[i]nformation that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations and government policies,'' excluding classified information. The NARA proposed CUI rule encompasses ''Controlled Technical Information'' as one of the *categories* of CUI recognized in the CUI Registry. *See* http://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html. Thus, the UCTI that DoD presently controls through its separate DFARS rule will come to be subsumed in the NARA rule that defines and categorizes and sets general safeguarding requirements for CUI.

 COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

either directly or through the use of managed services to satisfy CUI security requirements.

- NIST emphasizes that the many additional controls described in 800-53 are ''non-prescriptive'': While listed with the intent ''to promote a better understanding of CUI security requirements,'' 800-53 controls are ''not intended to impose additional requirements on nonfederal organizations.''[57]
- SP 800-171 recognizes that nonfederal organizations have specific safeguarding measures in place to protect their information that also may be sufficient to satisfy the CUI security requirements.
- By mapping of NIST 800-171 requirements to other regimes, such as ISO/IEC, NIST appears to recognize that many companies already rely on other standards and practices to achieve the security sought for CUI. NIST also offers guidance on how to locate equivalent controls for 800-171 with the core functions of its voluntary Framework.
- NIST explicitly recognizes that companies may choose to create separate security domains to handle and protect CUI without increasing the organization's ''security posture'' beyond what it needs for its core business or other operations.
- Because nonfederal organizations may lack the means to satisfy every CUI security requirement, NIST allows that they ''may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a particular requirement.''[58]

Measures that protect federal information when in contractor hands also will protect valuable contractor information where the controls are employed across an organization. The federal government and its contractors share an interest in protecting the confidentiality of contractor intellectual property against extraction or theft, whether by criminal organizations, business organizations, state-sponsored hackers or state actors. But that does not mean that the federal government should impose its security rules upon private companies beyond the information system and service domains of a company where CUI (or UCTI) are resident or utilized.

Industry undoubtedly will be concerned about the prospect that federal agencies will take the requirements of SP 800-171 as the ''floor'' and use tailoring to layer additional obligations upon them. Industry's concerns are natural and justified. As explained, NARA's proposed CUI rule does not resolve the question of whether and how agencies will insist upon higher levels of information safeguarding. Nor does the present draft of SP 800-171 resolve the question. Under the heading, ''The Requirements,'' SP 800-171 states:

> Additional CUI security requirements beyond those requirements described in this publication may be justified *only* when such requirements are based on federal law, regulation, or governmentwide policy and indicated in the CUI Registry as *CUI specified*. [sic] The provision of safeguarding requirements for CUI in a particular specified category will be addressed by NARA in its CUI guidance and in the CUI FAR; and reflected as specific requirements in contracts or other agreements.[59]

This language—presented in a footnote—begs the question because it is unaccompanied by any of the implementation particulars that would make it more useful guidance. NARA has published the CUI Registry, but it far from complete. NARA's proposed CUI rule expressly anticipates that agencies will determine additional security controls or dissemination constraints for categories or subcategories of CUI that are identified as ''*CUI Specified*.'' But the CUI Registry today contains no more than placeholders for this important content. Thus, even after NARA has published its proposed CUI rule, many important implementation details remain wholly conjectural.

The proposed SP 800-171 requirements will not have their intended effect, except perhaps as illustrations of potentially useful security practices, unless and until they are accompanied by *both* the final federal rule to define CUI *and* a new federal acquisition rule, of general application across all contracting, that will establish the methods and contract terms by which these requirements are imposed upon prospective federal contractors. Of this ''triad,'' the last two remain in gestation.

DHS Moves Out

This has not kept some federal agencies from moving out, nonetheless, with special measures to protect CUI that they consider of critical importance. DoD has made considerable progress with its UCTI regulations, first issued in November 2013. The Department of Homeland Security (DHS) recently issued a ''class deviation'' imposing a pervasive and highly demanding control regime on certain of its information when in the hands of its contractors.[60] If this is a precursor to what other agencies will do in the absence of a generally applicable federal acquisition approach, industry has cause for dismay.

The DHS Special Clause is to be used for existing as well as new ''high risk'' contracts where the contractor has access to ''sensitive information'' or its IT systems input, store, process or output such information. It is to be included in new solicitations, and DHS seeks to add the provision to existing contracts by bilateral modification.

The responsible DHS program manager is required to prepare a ''Requirements Traceability Matrix'' (RTM) when a contractor IT system is to be used with such sensitive information. That RTM is to be prepared in accordance with FIPS 199, meaning that security categorization will take into account the three objectives of confidentiality, integrity and availability as well as distinctions among ''impact'' levels. The RTM will generate the security controls that ''must be implemented on the contractor's IT system,'' and these controls are set at ''no less than 'Moderate' '' when a contractor's IT system will be used with sensitive information that includes Personally Identifiable Information (PII), Sensi-

[57] NIST SP 800-171 (Final Public Draft), at 8 & n.19.
[58] *Id.* at 5.
[59] *Id.* at 8 n.29.
[60] DHS Class Deviation 15-01 (3/9/15) for the ''Safeguarding of Sensitive Information,'' *available at* http://tinyurl.com/lh59ywp.

tive Personally Identifiable Information (SPII) or Sensitive Security Information (SSI).[61]

Where applied by contract, the clause obligates a contractor to follow multiple DHS-specific controls, policies and guidance. The contractor must receive an ''Authority to Operate'' and agree to and complete a ''Security Authorization Process'' which includes an independent third-party assessment. DHS insists upon a right to conduct ''random periodic reviews'' to ensure that the security requirements are met. Contractors subject to the Special Clause must afford broad audit access, and ''continuous monitoring'' requirements are imposed. Should there be a cyber event involving ''known or suspected sensitive information,'' the contractor must report ''within one hour of discovery.''[62]

On their face, these requirements are consistent with what might be expected to apply to ''federal information systems,'' and they appear to utilize processes (such as authorization to operate) drawn from the FedRAMP process that governs cloud security matters. However, the ''class deviation'' and the Special Clause do not appear to be limited just to companies who are under contract to DHS to operate federal information systems; rather, it seems to be the intent of DHS to apply these requirements to private contractors who have and use certain sensitive DHS information even if their access to or use of that information is through a nonfederal information system. If true, one can anticipate many industry objections because several of these requirements are onerous in part because they depart from customary norms even of private sector industry leaders. The requirements of DHS-specific authorization and DHS-directed third-party assessment, along with required audit access and monitoring, likely will generate objections as being unreasonably and unnecessarily costly and burdensome.

As illustrated by the new DHS initiative, important aspects of cyber supply chain requirements will be agency-specific. Agencies can tailor security controls to address the nature of information they protect and to reflect the risk of attack as well as the impact of loss of confidentiality. For low-risk situations involving information of relatively benign character, baseline controls could be tailored downward. Certainly, individual agencies have an interest in governing the reporting and response obligations that arise when a breach that affects the CUI of a particular agency occurs.

At the same time, if every agency imposes its own standard, and each agency applies its own oversight, the consequences could be impossibly disruptive and costly to many companies in the federal supply chain—especially to small businesses. Ultimately, though agencies will have the power to demand much of their suppliers, they cannot force companies to remain sellers in the federal marketplace. Some leading companies already refuse to sell directly to the federal government exactly because the unique federal compliance demands cannot be reconciled with their general, global business norms. In the end, the imposition of additional controls and risks will carry a price, and agencies will have to consider very carefully whether they can afford the price tag that would accompany imposition of unnecessary measures of prescription of NIST controls where other sufficient surrogates are in place.

[61] *Id.* at 4.
[62] *Id.* at 6.

Critical Missing Pieces

NARA is responsible to resolve *what* constitutes CUI that requires protection; its proposed rule recently entered the public comment period.[63] Apart from such important issues as the categorization, designation and safeguarding of CUI, the NARA CUI rule touches many other issues of broad public importance, such as public access to and the dissemination of federal information. These considerations alone suggest that the conclusion of the CUI rulemaking process may be more time-consuming than NARA may now expect.

SP 800-171 does not now differentiate among the sensitivity or significance of the various categories and subcategories of CUI. Nor do either the proposed CUI rule or SP 800-171 answer questions of what ''tailoring'' may be needed for CUI that agencies and NARA determine are to receive ''*CUI Specified*'' safeguards. All of these unknowns confront agencies, because those agencies will be uncertain whether their information is protected sufficiently, and the contractor community, which still does not know what costs and burdens to expect of heightened cybersecurity. These are very important considerations given the enormous volume and variety of CUI and the breadth of the potential application of federal cybersecurity controls to the commercial federal supply chain.

By definition, ''nonfederal information systems'' are those outside the boundaries of federal information systems. They may be systems of state and local governments, educational institutions, federal contractors and grantees, or those of other nongovernmental or even foreign organizations on which sensitive federal information (i.e., CUI) resides.

Thousands of nonfederal public and private sector enterprises host or use CUI, as it will be defined by the NARA CUI rule. They could become subject to the cybersecurity requirements of SP 800-171, and NARA is working (with the support of other federal agencies) on a FAR clause of general applicability that it intends will govern all federal agency purchases. The significance of this broad federal ''enterprise level'' initiative is potentially profound. As recognized by SP 800-171, the federal government relies upon nonfederal information systems and external information system service providers. When implemented by acquisition process and contract requirements, protecting that federal interest will impact the vast number of private companies that figure into the federal supply chain.

A Contractual Issue

That the federal government has important interests to protect, in the confidentiality of its CUI and UCTI, is inarguable. It is certain that other agencies will follow DoD's lead in imposing at least ''recommended requirements'' upon the information systems of contractors that store, use or transmit this information. NIST will be a primary source for the security controls. But these requirements are not self-imposing upon federal contrac-

[63] Executive Order 13556, *Controlled Unclassified Information*, issued Nov. 4, 2010, *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf, makes NARA responsible to develop and issue directives ''as are necessary'' to standardize how the executive branch handles unclassified information that requires safeguarding or dissemination controls. Information about NARA's effort is *available at* http://www.archives.gov/cui/.

 COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

tors. Rather, federal agencies will utilize the means of ''acquisition planning and contract administration'' to achieve the intended protection of the confidentiality of CUI.

Acquisition planning implicates many possibilities. Civilian agencies might require offerors to meet at least the minimum cyber controls of SP 800-171 as a condition of eligibility for the award of contracts that involve the use, transmittal or generation of CUI. Federal civil agencies could consider the presence of minimally sufficient cyber controls, as suggested by SP 800-171, as necessary to demonstrate a contractor is ''responsible'' and therefore eligible for award.[64] Agencies may seek demonstration of the adequacy of cyber controls and fashion evaluation criteria to award credit for comparatively superior controls. Contract clauses that will obligate companies to maintain security controls to NIST standards, or the equivalent, can be expected, and liability could be imposed if a cyber event occurs and a company is unable to show it took measures commensurate with the contract requirements.[65]

SP 800-171 focuses on systems to protect CUI. The present draft of SP 800-171 acknowledges its dependency upon the pending NARA CUI regulation to categorize, designate and mark CUI. Until the CUI rulemaking process is complete, SP 800-171 exists in a ''vacuum'' as to both *what* information is to be subject to controls and *how* industry is to be informed or self-determine whether information is subject to CUI controls. NARA has taken upon itself the task of producing a ''single Federal Acquisition Regulations (FAR) clause that will apply the requirements of the proposed [CUI] rule to the contractor environment.''[66] NARA has ambitions to get this accomplished within 2015, an objective that could prove more ambitious than realistic, given the complexities involved. In the absence of such a single rule, however, many agencies may proceed to act independently and individually, following the lead of DoD and more recently DHS. They will be motivated by perception of the cyber vulnerability of commercial ICT systems and worry over the consequences if confidentiality of their CUI is lost.

Even without the ''single FAR rule'' that NARA contemplates, agencies can employ NIST SP 800-171 to assist in their ''acquisition planning,'' as a basis for contractually required CUI cyber safeguards, and for ''contract administration'' measures. An approach utilizing SP 800-171 would be a responsible and informed way for agencies to improve their assurance of contractor cyber protection without risking overreach or demanding cyber control practices at odds with even best commercial norms. SP 800-171 is intended to require contractors to safeguard CUI, but it recognizes both the existence and suitability of cyber control strategies and methods that do not require direct implementation of NIST's SP 800-53 controls that were fashioned for federal information systems.

Until CUI is defined, a control regime is articulated *and* acquisition mechanisms are in place, neither the government nor industry will know what information is subject to the safeguarding requirements, whether or which cybersecurity requirements apply or what contractual duties (or liabilities) accompany the cybersecurity obligations.[67]

Reporting Cyber Incidents

Absent from SP 800-171 are specific instructions for reporting of cyber incidents.[68] The importance of improved cyber reporting has drawn much public attention recently, as evidenced by the White House Summit on Cybersecurity and Consumer Protection held Feb. 13 at Stanford University. At the summit, Obama signed new Executive Order 13691, effective immediately, to promote improved information sharing about cyber threats, both within the private sector and between the government and the private sector.[69] The further evolution of SP 800-171 and companion implementation measures surely will address reporting of cyber attacks that affect CUI on nonfederal information systems.

SP 800-171 makes little reference to NIST's ''Framework for Improving Critical Infrastructure Cybersecurity,'' beyond offering guidance on how to use ''mapping tables'' to relate the controls required by SP 800-171 to counterparts in the five families of controls in the Framework. This seems odd because the Framework

[64] The policy of the federal government is to limit awards to ''responsible'' prospective contractors only. FAR 9.103(a). A purchase or award cannot be made unless there is an affirmative determination of responsibility. *Id*. at 9.103(b). A prospective contractor must affirmatively demonstrate its responsibility including, when necessary, the responsibility of its subcontractors. *Id*. at 9.103(c). GSA recently signaled that it may take a more aggressive approach to assessment of contractor responsibility. On Dec. 12, 2014, GSA issued a request for information that comments: ''Federal buyers need better visibility into, and understanding of, how the products, services, and solutions they buy are developed and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of those products and services.'' RFI BizDueDil-RFI-001, ''Business Due Diligence for Acquisitions Involving Government Information or Information Systems,'' *available at* http://tinyurl.com/lwjmq3j.

[65] DoD's UCTI DFARS contract clause, DFARS 252.204-7012(b), states that contractors subject to the clause ''shall provide adequate security'' to safeguard UCTI from compromise and mandates an information systems security program that implements specified controls from SP 800-53 unless an exception is justified or an alternative is used. In the event of a cyber event, an audit or investigation may follow. A claim of breach could arise if the government were to conclude that the cyber event could have been avoided through use of controls that meet the NIST requirements.

[66] 80 Fed. Reg. 26,503.

[67] In contrast, the DFARS addresses ''definition'' and ''designation'' of UCTI by reference to ''distribution statements'' in DoD Instruction (DoDI) 5230.24 that inform the controlling DoD component (and DoD contractors) of how to determine whether information is UCTI. DoD issued Program Guidance and Instruction (PGI) Dec. 16, 2014, which further answers implementation questions. Many federal contractors to DoD also serve nondefense federal agencies. Some will employ a common information system to hold CUI and UCTI. Where prudent, consistency should be sought among federal agencies in the information assurance and cybersecurity measures they impose upon all forms of CUI (including UCTI) in nonfederal information systems.

[68] In contrast, DFARS 252.204-7012(d) contains extensive reporting requirements and would standardize reporting procedures when a ''cyber incident'' occurred. Such an incident is defined as ''actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.''

[69] Executive Order, ''Promoting Private Sector Cybersecurity Information Sharing,'' 2/13/15, *available at* http://tinyurl.com/nzmejd9 (14 PVLR 324, 2/23/15).

was developed in collaboration with industry to assist organizations, voluntarily, to adopt and apply risk-based measures to manage their cybersecurity risk. In the Framework, NIST observed that organizations ''will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices in the Framework will vary.''[70]

The same propositions hold true for the agencies whose CUI merits protection and for the private sector enterprises that may become subject to SP 800-171 controls. Similar risk-informed flexibility should guide the expectations and demands of individual federal agencies and their oversight. Informed forbearance from dictated controls, unnecessary oversight or administrative obligation or unreasonable demands will reduce compliance and implementation burdens on federal contractors.

[70] Framework, n.12.

Conclusion

The federal supply chain includes companies that are entrusted with federal information. The ICT systems of these companies are at constant risk of cyber attack. Considering the threat, and the national interest in protecting the many categories of sensitive federal information, it is necessary and proper for civilian federal agencies to use their authority over acquisition methods and contract requirements to improve cybersecurity and information assurance of nonfederal information systems. These measures should be taken only after the government is able to determine and designate the information to be protected, with due regard for the sensitivity of information and the consequences of its release or compromise, and with recognition of the diversity of companies affected and the presence of responsible choices among available cybersecurity controls.

 COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423