Bloomberg BNA

Daily Report for Executives™

Cybersecurity

The federal supply chain includes companies that are entrusted with federal information. The information and communications technology systems of these companies are at constant risk of cyber attack, making it necessary for civilian federal agencies to use their authority over acquisition methods and contract requirements to improve cybersecurity and information assurance of nonfederal information systems. Author Robert Metzger flags the key issues to resolve as new initiatives seek to build efficient, practicable defenses.

Cybersecurity and Acquisition Practices: New Initiatives to Protect Federal Information of Civilian Agencies

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]

[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 communication 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 should not be attributed to any client of Rogers Joseph O'Donnell or to any organization with which Mr. Metzger is or may be affiliated.*

Cyberthreats are posed to information and communication 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, is destroyed, compromised or stolen. Consequences include impairment of government and private sector functions and loss or corruption of sensitive and proprietary data. Privacy interests of citizens can be injured where a cyberattack compromises the confidentiality of federal records that contain, for example, personal identification information, health information or tax records.

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 regu-

[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.

 ISSN 0148-8155

larly 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 electronic, electronic or electro-mechanical 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 cloud infrastructure and web-enabled delivery, threats to information systems may be 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 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, the presence of security controls is problematic, at best.

With limited exceptions, no statute or regulation generally obligates federal nondefense contractors to protect against threats to the supply chain.

With limited exceptions,[5] no statute or regulation generally obligates federal nondefense contractors to protect against threats to the supply chain, specifically *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. 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, federal civil functions are 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 who 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] While the final definitions are not in place, CUI will encompass information in such diverse categories as technical information with military or space application (unclassified controlled technical information or UCTI), copyrights, critical infrastructure, emergency management, export control, financial, geospatial, immigration, intelligence (*e.g.*, financial records, Foreign Intelligence Surveillance Act), law enforcement, legal, NATO, patent, privacy (including health information), proprietary business records and SAFETY Act (anti-terrorism related) information.[10]

[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.

[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); 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. 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 is very much a work-in-progress. As to ''safeguarding obligations,'' it presently invokes four documents (FIPS 199, FIPS 200, NIST SP 800-53 rev.4 and NIST 800-60, rev. 1) that explicitly do *not* apply other than to information within the federal government. Yet, the CUI Registry enumerates many categories and subcategories of information that reside regularly on ''nonfederal informa-

  DER ISSN 0148-8155

CUI stored, used or communicated through private (nonfederal) ICT systems must be protected against cyberthreats. 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.

Crucial Questions. The National Institute of Standards & Technology (NIST) is working now to complete SP 800-171, a control regime to protect CUI on nonfederal information systems.[11] Several crucial questions are yet to be resolved, however. The first is definitional. For years, the federal government has struggled to reconcile conflicting definitions of CUI.[12] It will not be practicable to impose security controls to protect CUI if neither agencies nor companies know what it is.

The National Archives and Records Administration (NARA) has been assigned the responsibility to promulgate the regulations needed to resolve this uncertainty. On May 8, 2015, 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 of Federal Regulations.[13] A central feature of the rule is the use of the ''CUI Registry'' to identify 23 discrete categories and 82 subcategories of CUI. Examples of these categories include, for illustration, ''Controlled Technical Information,'' ''Critical Infrastructure,'' ''Emergency Management,'' ''Financial,'' ''Intelligence,'' ''Law Enforcement,'' ''Legal,'' ''Patent,'' ''Privacy'' and ''Proprietary Business.'' (These categories speak to both the government and private sector interest in assuring confidentiality of CUI against unauthorized compromise.) The proposed rule sets a basic ''safeguarding'' standard for CUI, but provides for enhanced (or different) ''specified'' safeguards for certain categories or subcategories, as will be elaborated in the Registry as it evolves. As explained in the announcement of the proposed rule, NARA has partnered with NIST to develop a special publication—SP 800-171—to articulate information security practices that will be suitable to adapt in the contractor environment in order to protect CUI. The proposed rule also assigns to agencies the responsibility to designate and mark CUI.

While the NARA CUI rule is not final, one can anticipate tension between the ''gatekeeper'' role that NARA seeks to play and the disposition of federal agencies to determine by and for themselves which of their information requires what level of security controls. The NARA rule elects to treat all CUI at the confidentiality impact level of ''moderate'' in accordance with FIPS 199. Conceivably, some agencies will conclude that certain of their CUI requires a higher level of security. This is likely to be addressed by ''tailoring'' controls upward through specific contract requirements, but as agencies do so they work against one of the other goals of the NARA effort, namely a common set of practices both to designate and protect CUI.

Agencies are in the best position to assess the impact to their operations should their CUI suffer loss of confidentiality. They also will need to consider that elevated CUI controls may constrain their access to commercial market technologies, reduce competition and increase their costs of supplies and services. For these reasons, each federal agency will need to weigh carefully where and how to change and use acquisition practices and contract requirements to encourage federal contractors to adopt new security controls as NIST may recommend. NARA has a leadership role to designate CUI and to establish the strategy for its protection, but implementation of its objectives necessarily involves interagency coordination as well as individual agency initiatives.

As concerns the CUI controls, NIST's job is far from done. SP 800-171 today seeks only to protect the ''confidentiality'' of information in nonfederal systems.[14] The same information, if held in a federal information system, is subject to FIPS 199—which seeks to protect ''integrity'' as well as ''availability'' of that information. SP 800-171 treats all CUI in nonfederal information systems as equivalent in terms of the ''impact'' of the security objectives. In contrast, the same CUI, if held in a federal information system, is subject to FIPS 200—which distinguishes among ''low,'' ''moderate'' and ''high'' impact and directs increasing levels of controls accordingly.

Boundary-Setting Problems. This seeming paradox points to another analytic problem, namely the pervasive difficulty, in an interconnected world, of setting control boundaries for ''federal information systems'' as distinct from ''nonfederal'' or ''external'' information systems.[15] In SP 800-171, NIST articulates a special and reduced subset of security controls for ''nonfederal information systems.'' 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

---

tion systems'' as well as ''external information systems.'' These are defined in n.10, *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.

[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.

[13] 80 Fed. Reg. 26,501 (May 8, 2015).

[14] SP 800-171 (Final Public Draft), at 2.

[15] 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.

measures imposed upon the federal supply chain. Those costs may be higher prices for supply or services or lost access to sources that choose not to accommodate the federal demands. Means must be found to achieve the objectives of NIST's control regime without denying or superseding the validity of other strategies and techniques as may be sufficient, but different.

The Cyberthreat to Federal Information—and Citizen Privacy.

The cyberthreat is 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, disrupted day-to-day operations and the release of supposedly ''private'' information caused great embarrassment. The attack on Anthem Inc. apparently compromised 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 the nondefense public sector 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 healthcare 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.''[16]

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.''[17]

This report confirms that the cyberthreat extends to federal information systems[18] 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),[19] the Federal Information Processing Standards (FIPS), Federal Risk and Authorization Management Program (FedRAMP),[20] Office of Management and Budget (OMB) Circular No. A-130,[21] and the work of NIST. Particularly notable is NIST SP 800-53 (''Security and Privacy Controls for Federal Information Systems and Organizations''), rev. 4, which updates and categorizes standards and guidelines for federal cyber controls, excepting national security sys-

[16] SP 800-171 (Final Public Draft), at 1.

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

[18] ''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.

[19] 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 Federal Information Processing Standards (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.

[20] 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.

[21] 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.

  DER ISSN 0148-8155

tems.[22] and the Cybersecurity Framework, Version 1.0 (''*Framework*''),[23] 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.[24] 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 invoked *by agencies* in the acquisition process (as necessary qualifications, for example), as part of competitive selection (in evaluation criteria) or imposed by 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.[25]

Through issuance of Executive Order 13636 (''Improving Critical Infrastructure Cybersecurity''), President Barack Obama has encouraged voluntary adoption of cybersecurity measures to protect critical infrastructure.[26] 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*.''[27]

Federal Market Power. That the federal government is expected to spend $90 billion on IT in FY 2016 suggests it has market power sufficient to steer its supply chain to improve cybersecurity measures. Similarly, the very large companies who often control or operate critical infrastructure also should have sufficient influence over their supply chain to obtain improved cyber and supply chain protection.[28]

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. 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.[29] 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.''[30] Through the required solicitation provisions and contract clauses, these regulations impose 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, a Joint Working Group on Improving Cybersecurity and Resilience through Acquisition was formed by DoD and GSA. The final report of the Joint Working Group was released January 23, 2014.[31] 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 improved supply chain security measures. Some may question whether such federal ''inter-

[22] NIST SP 800-53, rev.4, *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[23] ''Framework for Improving Critical Infrastructure Cybersecurity,'' v. 1.0 (2/12/14), *available at* http://www.nist.gov/cyberframework/. 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.

[24] 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. Cloud information services are delivered through use of ''external information systems.''

[25] 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.'' NIST SP 800-37, at I-1.

[26] Executive Order 13636 (Feb. 12, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. 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.

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

[28] 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 cyberthreats 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.

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

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

[31] *Improving Cybersecurity and Resilience through Acquisition*, *available at* http://tinyurl.com/kfuau32.

vention'' 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 risk to federal interests should the confidentiality of sensitive federal information be lost or compromised 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.

NIST SP 800-171.

NIST SP 800-171 was first released in draft, for comments, November 18, 2013.[32] The Final Public Draft was released in April 2015. Its purpose is to protect the *confidentiality* of sensitive federal information (namely, CUI) that resides on the *nonfederal* information systems of contractors or other organizations. In contrast, for *federal* information systems, FISMA defines not one but *three* security objectives for information and information systems: confidentiality, integrity and availability.[33] Another departure is the complete absence from SP 800-171 of any distinction to recognize relative *impact* of a security breach upon an organization or individuals. This, in contrast, is a core tenet of FIPS 199. Information and information systems are categorized 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.''[34]

Importantly, FIPS 199 makes the determination of security categorization also a function of the ''information type,'' distinguishing among such types as ''public information'' (non-sensitive) or ''investigative information'' (very sensitive), and then examining impact as to *each* of the *three* security objectives (confidentiality, integrity and availability).[35] NIST SP 800-171, in contrast, does not discriminate among ''information types'' in setting security objectives. All CUI is treated as though it has the same sensitivity and no CUI receives a different control outcome as a function of *impact* in the event of a breach.[36]

Three Assumptions. As presently proposed, SP 800-171 makes three ''assumptions'' which explain, albeit briefly, these ''departures'' from the rules which apply to CUI on federal information systems.[37] One assumption is that statutory and regulatory requirements for the protection of CUI are ''consistent,'' whether the information resides in federal or nonfederal information systems. Another 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.

These assumptions are not well supported. Even if the requirements for protection of CUI are the same, the safeguards to protect CUI are not the same for federal as for nonfederal information systems. (As will be explained, for non-federal information systems NIST proposes to apply a lesser subset of the ''moderate'' control baseline of SP 800-53 that would apply to the same information in federal information systems. As to the stated assumption that the ''impact'' value is no lower than ''moderate,'' this seems to commoditize the many variations of CUI (recognized in the NARA Registry) and to homogenize likely differentials in true impact that exist in fact.

The departures from the FIPS norms and SP 800-53 control baselines appear to be in the nature of ''concessions'' that NIST has adopted in order to articulate (or rationalize) a recommended extension of *some* federal controls outside their present domain of federal information systems to the very much larger realm of nonfederal systems as may be operated by private sector contractors, state and local governments and educational institutions. One can appreciate restraint in trying to impose the federal system outside its original boundaries. However, there have been losses in translation. For example, FIPS 199 and FIPS 200 work in combination to adjust the level of controls required to the impact of a cyber event as affects the distinct security objectives of confidentiality, integrity and availability. This is essentially absent from SP 800-171 (at least in the Final Public Draft) and it deprives potential adopters (and contracting agencies) from a toolset that could help to inform risk-based decisions on control levels.

With respect to security requirements, SP 800-171 claims a ''well-defined'' structure that consists of ''a *basic* security requirements section'' and a ''*derived* security requirements section.''[38] The former is obtained from FIPS 200 while the later are derived from the security controls in NIST SP 800-53, starting from the

[32] 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.

[33] 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.'' While this is true, as any measure to protect confidentiality will have some benefit to improve assurance of both integrity and availability, NIST never addresses squarely why recommended controls for CUI in nonfederal systems exclude these security objectives.

[34] 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.

[35] *Id*. at 3.

[36] 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.

[37] *Id*. at 5.

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

  DER ISSN 0148-8155

''moderate'' controls baseline but reducing the controls through ''tailoring'' 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. In the Final Public Draft, SP 800-171 describes fourteen (14) families of security requirements (including both ''basic'' and ''derived''), in contrast to the 17 families of SP 800-53.[39] 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 distinct from but are ''mapped'' identify relationship to counterparts 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 ''low'' baseline—though more than DoD presently applies in its counterpart rule to protect UCTI:

References to NIST SP 800-53 Controls[40]

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 between control requirements of SP 800-171 to counterparts in SP 800-53. SP 800-171 (in the Final Public Draft) states 14 families of security requirements. (These are Access Control; Awareness & Training; Audit & Accountability; Configuration Management; Identification & Authentication; Incident Response; Maintenance; Media Protection; Physical Protection; Personnel Security; Risk Assessment; Security Assessment; System & Communications Protection; and System and Information System Integrity.) For each of these 14 families, NIST articulates both a ''Basic Security Requirement'' and whether there are ''Derived Security Requirements.'' 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. Each of the fourteen families also contains references to relevant controls or control enhancements from SP 800-53, but those references are for information but not mandatory. In other words, reference in the Requirements section of SP 800-171 to one (or many) SP 800-53 controls and enhancements does not mean that satisfaction with the SP 800-171 requirement can be achieved only if the referenced SP 800-53 control is met.

Coordination, if not reconciliation, with DoD will be necessary. Through its 2013 regulations on UCTI, DoD already has acted to impose limited security controls on its contractors who host, use or transmit sensitive but unclassified technical information with military or space application. However, the UCTI regulations invoke just 51 cyber controls,[41] also drawn from SP 800-53. An important goal of federal authorities should be to examine carefully what constitutes a sufficient level of controls and to 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.

Non-recurring implementation costs and recurring system operation costs rise with the level of controls. While there are notional benefits to a uniform standard, for all federal contractors, addressing all CUI and UCTI, further assessment may indicate that a lesser set of controls is the cost-effective choice for a baseline that is to be broadly applicable. Agencies can add levels of controls by project, procurement, statement of work or special contract provision. These can be derived from controls in SP 800-53's extensive catalog—but the private sector should be enabled if not encouraged to demonstrate adequate alternatives as NIST is not unique in documentation of cybersecurity best practices.

Both UCTI and CUI similarly concern unclassified but sensitive federal information.[42] Even though there is distinct national defense significance to UCTI, the eventual federal regulatory regime likely will recognize that there is rough parity in the importance of federal interests in protecting UCTI vis-a-vis CUI. This proposition points towards convergence of the UCTI and CUI regulatory regimes. Conceivably, if a broad federal rule is implemented through the FAR, to protect CUI using controls as will be recommended by SP 800-171 in its final form, the present DFARS may become a subset of or subsumed by the CUI rule.

Implications for NIST's 800-171 Controls 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 they 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 accomplished with-

[39] 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.

[40] *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.

[41] The DFARS UCTI rules reference just 51 of the SP 800-53 controls. 78 Fed. Reg. 69,281.

[42] ''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.

out 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 controls are tailored down significantly from what would be applicable from the SP 800-53 ''moderate'' baseline.
- NIST allows that nonfederal organizations can implement a variety of potential security solutions 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 these are ''intended to promote a better understanding of CUI security requirements,'' they are ''not intended to impose additional requirements on nonfederal organizations.''[43]
- SP 800-171 recognizes that nonfederal organizations have specific safeguarding measures in place to protect their information which may also be sufficient to satisfy the CUI security requirements.
- By mapping of NIST controls and families 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 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.''[44]

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 has an interest in protecting the confidentiality of contractor intellectual property against extraction theft, whether by criminal organizations, business organizations, state-sponsored or state actors. But that does not mean that the federal government should impose its security architecture upon private companies beyond the information system and service domains where CUI (or UCTI) are resident or utilized.

[43] NIST SP 800-171 (Final Public Draft), at 8 & n.19.
[44] *Id*. at 5.

Industry undoubtedly will be concerned about the prospect that federal agencies will take the controls required by SP 800-171 as the ''floor'' and layer additional obligations upon them.

Industry undoubtedly will be concerned about the prospect that federal agencies will take the controls required by SP 800-171 as the ''floor'' and layer additional obligations upon them. Today, there is not even a proposed FAR rule to examine, as to the application of CUI security controls. Industry's concerns are natural and justified. Little comfort can be found in the present final draft of SP 800-171, not because the subject is ignored, but because it is dealt with as a virtual afterthought. 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*. 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.''[45]

This language—presented in a footnote—is unaccompanied by any of the implementation particulars that would give it significance. NARA has published the CUI Registry but it is not complete. While NARA's proposed rule will help establish workable definitions of what constitutes ''CUI,'' the rule is not yet final and we may find issues surface only after implementation. As the CUI Executive Agent, NARA has to set the ''governmentwide policy'' on imposition of additional controls. While the proposed rule eliminates some of the mystery, many questions remain and should be considered carefully by industry stakeholders. For example, 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 details remain conjectural.

The proposed SP 800-171 controls have no effect, except perhaps as illustrations of potentially useful security practices, unless and until they are accompanied by *both* the expected new 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.

[45] *Id*. at 8 n.29.

  DER ISSN 0148-8155

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. The Department of Homeland Security (DHS) recently issued a ''class deviation'' imposing a pervasive and highly demanding control regime on certain of its information in the hands of its contractors.[46] If this initiative 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, output or store 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), Sensitive Personally Identifiable Information (SPII) or Sensitive Security Information (SSI).

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 obtains 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.''

On their face, these requirements are consistent with what might be expected to apply to ''federal information systems'' and they appear to draw upon 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 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.

If every agency imposes its own standard, and each agency applies its own oversight, the consequences could be impossibly disruptive and costly.

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 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 as arise when a breach occurs that affects the CUI of a particular agency.

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.

Critical Missing Pieces

SP 800-171 does not resolve *what* constitutes CUI that requires protection.[47] Nor does it differentiate among the sensitivity or significance of such data as might inform agencies when the costs and burdens of heightened cybersecurity are justified. These are very important considerations given the breadth of potential application of federal cybersecurity controls to the broad federal supply chain.

By definition, ''nonfederal information systems'' are those outside the boundaries of federal information sys-

[46] DHS Class Deviation 15-01 (3/9/15) for the ''Safeguarding of Sensitive Information,'' *available at* http://tinyurl.com/lh59ywp.

[47] Executive Order 13556, *Controlled Unclassified Information*, issued on Nov. 4, 2010, *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf, makes the National Archives and Records Administration (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/.

tems. They may be systems of state and local governments, educational institutions, federal contractors and grantees, or those of other organizations on which sensitive federal information (i.e., CUI) resides.

Thousands of nonfederal public and private sector enterprises host or use CUI that could become subject to the cybersecurity controls that SP 800-171 will require. SP 800-171 is accompanied by an architecture by which CUI will be defined and made subject to regulations expected to 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. Protecting that federal interest will impact the vast number of private companies who 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 who 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 contractors. Rather, federal agencies will utilize the means of ''acquisition planning and contract administration'' to achieve the intended protection of the confidentiality of CUI.

As concerns acquisition planning, civilian agencies may require offerors to meet at least the minimum cyber controls of SP 800-171 as a condition of eligibility for award of contracts that involve use, transmittal or generation of CUI. Federal civil agencies may come to 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.[48] Contract clauses can be expected that will obligate companies to maintain security controls to NIST standards, or equivalent, 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.[49]

SP 800-171 focuses on systems to protect CUI, and NARA is at work to define and categorize CUI so that federal contractors will know what must be protected. The present draft of SP 800-171 acknowledges its dependency upon the NARA regulation. While NARA's proposed rule now is out for public comment (due July 7), it is not final. Until the 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. Indeed, SP 800-171—once it is finalized—affects contractor security practices only if and to the extent it is applied by contractual measure. We can expect DoD to revise its existing DFARS to adopt SP 800-171 to protect the Pentagon's UCTI (a species of CUI). When and how other agencies will follow suit is to be determined. 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.'' 80 C.F.R. 26503. While NARA has ambitions to get this accomplished within 2015, this could prove more ambitious than realistic.

Thus, SP 800-171 also depends upon specific ''acquisition planning'' and ''contract administration'' measures in order for agencies to achieve its cyber protection objectives for the federal supply chain. Until CUI is defined, a control regime is articulated and acquisition mechanisms are in place, neither the government nor industry will know whether or which NIST controls requirements apply, or what information is subject to the requirements, or what contractual duties (or liabilities) accompany the cybersecurity obligations.[50]

Reporting Cyber Incidents. Absent from SP 800-171 are specific instructions for reporting of cyber incidents.[51] 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 on February 13, 2015 at Stanford University. At the Summit, the President signed a new Executive Order, effective immediately, to promote improved information sharing about cyber threats, both within the private sector and between government and

[48] 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.

[49] 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 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.

[50] In contrast, the DFARS addresses ''definition'' and ''designation'' of UCTI by reference to ''distribution statements'' in 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) on Dec. 16, 2014, which further answers implementation questions. Many federal contractors to DoD also serve non-defense federal agencies. Some will employ a common information system to hold CUI and UCTI. Where possible, consistency should be sought among federal agencies in the information assurance and cybersecurity measures they impose upon UCTI and CUI in nonfederal information systems.

[51] In contrast, DFARS 252.204-7012(d) contains extensive reporting requirements and would standardize reporting procedures when a ''cyber incident'' occurs. 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.''

  DER ISSN 0148-8155

the private sector.[52] 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* 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.''[53]

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

Conclusion.

The federal supply chain includes companies that are entrusted with federal information. The information and communications technology 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.

---

[52] Executive Order, ''Promoting Private Sector Cybersecurity Information Sharing,'' 2/13/15, *available at* http://tinyurl.com/nzmejd9.

[53] *Framework*, n.12.