Bloomberg BNA

Federal Contracts Report™

Cybersecurirty

Cybersecurity for the Rest of Us: Protecting Federal Information of Civilian Agencies

BY ROBERT S. METZGER

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

Cyber threats 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.

The supply chain for ICT systems has many points of vulnerability. While the threats differ and the attack vectors are diverse, vulnerability is present at all levels, from device through equipment, and includes firmware and software. The global nature of the information technology supply chain contributes to the proliferation of these risks.

With limited exceptions,[3] no statute or regulation generally obligates federal non-defense contractors to

[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/.

Rogers Joseph O'Donnell, P.C. 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 Washington, D.C. office of the firm. This article presents the individual views of Mr. Metzger and should not be attributed to any client of Rogers Joseph O'Donnell, P.C., or to any organization with which Mr. Metzger is or may be affiliated.

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

[3] 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, NASA, and to the National Science Foundation. The same language also is 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

 ISSN 0014-9063

protect specifically against three types of threats to the supply chain: *physical* threats, such as posed by counterfeit electronic parts; *cyber-physical* threats, as represented by maliciously encoded electronic parts; and *cyber* threats as are posed to ICT systems. As explored in my previous articles,[4] DoD has taken initiatives, using its acquisition authority, to address its supply chain risk in all three areas.[5]

Corresponding action has not yet been taken on the civil side of federal contracting.[6] Yet, federal civil functions are exposed to substantially the same or similar risks. Federal agencies apply a variety of cyber security controls to contractors who operate ICT as ''federal information systems.''[7] 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 non-defense federal information. There are many categories of such information, which collectively constitute ''controlled federal information'' or ''CUI.''[8] While the final definitions are not in place, CUI will encompass information in such diverse categories as technical information with military or space application (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.[9]

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.

NIST, a unit of the Department of Commerce is now working to develop, through proposed SP 800-171, a control regime to protect CUI on nonfederal information systems.[10] 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.[11] It will not be practicable to impose security controls to protect CUI if neither agencies nor companies know what it is. Second, the federal agencies must determine how to change and use acquisition practices and contract requirements to cause federal contractors to adopt these security controls. As concerns the controls themselves, NIST needs to consider whether to recommend tiers or a single set of minimum controls for CUI, and how to employ the voluntary cybersecurity ''Framework'' (discussed below) as a basis for CUI protection. Agencies must consider whether they will insist upon adoption of NIST controls or accommodate reliance on other commercially accepted security practices.

The Cyber Threat to Federal Information. The cyber threat is very much in the public mind. Most of the publicized attacks have been against the private sector. The hack of Sony Pictures brought down that company's in-

agency has (1) reviewed the supply chain risk against criteria developed by the National Institute of Standards and Technology (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.

[4] *See* ''View From RJO: DOD's Cybersecurity Initiative - What the Unclassified Controlled Technical Information Rule Informs Public Contractors About the New Minimums in Today's Cyber-Contested Environment,'' Bloomberg BNA *Federal Contracts Report*, 102 FCR 744, Dec. 30, 2014 (Lucas T. Hanback, co-author); ''Convergence of Counterfeit and Cyber Threats: Understanding New Rules on Supply Chain Risk,'' Bloomberg BNA *Federal Contracts Report*, 102 FCR 744, Dec. 30, 2014 (Lucas T. Hanback, co-author) 101 FCR 167 (Feb. 18, 2014).

[5] 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.'' Department of Defense, ''Assured Microelectronics Policy,'' (July 2014), *available at* http://www.acq.osd.mil/se/docs/DoD-Assured-Microelectronics-Policy-RTC-July2014.pdf.

[6] NIST has released two drafts of Special Publication (SP) 800-161 (''Supply Chain Risk Management Practices for Federal Information Systems and Organizations''), *available at* http://csrc.nist.gov/publications/drafts/800-161/sp800_161_2nd_draft.pdf. A final version is expected soon. SP 800-161 recognizes that the ICT supply chain is a ''complex, globally distributed, and interconnected ecosystem'' which increasingly relies upon commercial available or open source products. SP 800-161 will provide federal agencies with guidance and controls, recommended for use with ''high impact systems'' to protect against ICT supply chain risks that include ''insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing''.

[7] 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 Appendix A, p.7.

[8] Executive Order 13556 of November 4, 2010, ''Controlled Unclassified Information,'' *available at* http://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information. 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.

[9] The NARA website presents information about CUI Categories and Subcategories, *available at* http://www.archives.gov/cui/registry/category-list.html#categories.

[10] NIST SP 800-171 (''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations''), Initial Public Draft (Nov. 2014), *available at* http://csrc.nist.gov/publications/drafts/800-171/sp800_171_draft.pdf.

[11] 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 www.archives.gov/cui/faqs.html*.

  FCR ISSN 0014-9063

formation systems, disrupted day-to-day operations and the release of supposedly ''private'' information caused great embarrassment. The attack on Anthem 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., E.U. and Russia. Those attacks warn that similar vulnerabilities are present in the non-defense 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.

There is official recognition of the serious and growing threat to government systems. The 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.[12]

This report confirms that the cyber threat extends to federal information systems[13] operated by as well as 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),[14] the Federal Information Processing Standards (FIPS), Federal Risk and Authorization Management Program (FedRAMP),[15] OMB Circular A130,[16] and the work of NIST. Particularly notable NIST publications include NIST SP 800-53, Rev. 4, which establishes standards and guidelines for federal cyber controls, excepting national security systems,[17] and the Cybersecurity Framework v. 1.0,[18] 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 necessarily extend to *nonfederal information systems*. The boundaries between ''federal'' and ''nonfederal'' information systems can be hard to distinguish.[19] 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.

Through issuance of Executive Order 13636 (''Improving Critical Infrastructure Cybersecurity''), the President has encouraged voluntary adoption of cybersecurity measures to protect critical infrastructure.[20]

---

[12] ''High-Risk Series: An Update,'' Report GAO-15-290 (Feb. 11, 2015), *available at* http://www.gao.gov/products/GAO-15-290.

[13] ''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. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems. *See* NIST SP 800-53, Rev. 4 (''Security and Privacy Controls in Federal Information Systems and Organizations'') (Apr. 2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[14] GSA explains ''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), National Institute of Standards and Technology (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.

[15] 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.

[16] 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.

[17] NIST SP 800-53, Rev. 4, n.8.

[18] ''Framework for Improving Critical Infrastructure Cybersecurity,'' v. 1.0 (Feb. 12, 2014), *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 private sector companies to employ across critical infrastructure sectors.

[19] 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 Apply 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.

[20] 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

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*.'' (Emphasis added).

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.[21]

DoD, which has the largest 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.

■ The Defense Federal Acquisition Supplement (DFARS) now states requirements to detect and avoid counterfeit electronic parts that are imposed on DoD's largest suppliers through mandatory contract clauses contained in solicitations for new supplies and services.[22] Large defense contractors who are formally ''covered'' by the DFARS are obligated to flow down the anti-counterfeit requirements to their entire supply chain – including commercial sources and small businesses. In addition, DoD utilizes purchasing system reviews to examine the adequacy of contractor systems to detect and avoid counterfeit electronic parts.

■ DFARS regulations on Unclassified Controlled Technical Information (UCTI) use acquisition methods (contract clauses and flowdown requirements) to impact all companies in its supply chain.[23] 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 FAR part 12 procedures for the acquisition of commercial items.''[24] 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 on January 23, 2014.[25] 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 ''intervention'' is necessary. Market forces (and enterprise self-protection) will 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 sensitive federal information be lost or compromised by reason of cyber breaches. Recent events in the private sector vividly demonstrate the costly, lasting injury that is the consequence of a successful cyber-attack even upon supposedly well-protected systems engaged in sensitive areas of commerce.

NIST SP 800-171. NIST SP 800-171 was released in draft, for comments, on November 18, 2013.[26] The comment period closed in January 2015. SP 800-171 seeks to protect sensitive federal information (namely, CUI) that resides on the *nonfederal* information systems of contractors or other organizations. SP 800-171 seeks uniformity in how federal agencies will protect their information by measures to be imposed on contractors or organizations. SP 800-171 distinguishes between ''basic'' and ''derived'' security requirements. The former is to eliminate requirements that do not need additional measures, such as functions that are primarily the responsibility of the federal government. The ''derived'' security requirements at the heart of the publication are selected from among security controls enumerated in NIST SP 800-53, starting from its ''Moderate'' security control baseline.

If finalized without material change, the effect of SP 800-171 will be to provide, for *all* federal agencies, a set of baseline controls the agencies may choose to impose upon *all* contractors who possess or transmit CUI on nonfederal information systems. The level of controls presently chosen is that of the ''Low'' Baseline of SP 800-53. Coordination if not reconciliation with DoD will be necessary. Through its 2013 regulations on UCTI,

---

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.

[21] 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.

[22] DFARS: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055), 79 Fed. Reg. 26092 (May 6, 2014).

[23] DFARS: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039), 78 Fed. Reg. 69273 (Nov. 18, 2013).

[24] DFARS 204.7303, at 79 Fed. Reg. 69280.

[25] *Improving Cybersecurity and Resilience through Acquisition*, *available at* http://www.gsa.gov/portal/content/176547.

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

  FCR ISSN 0014-9063

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, all drawn from SP 800-53 – less than half the number (115) that would be required by the SP 800-53 ''Low'' baseline that also is used in SP 800-171 for CUI.[27] 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. Non-recurring implementation costs and recurring system operation costs rise with the level of controls. While there are benefits to a uniform standard, for all federal contractors, 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.

Both UCTI and CUI similarly concern unclassified but sensitive federal information.[28] Even though there is distinct national defense significance to UCTI, the eventual regulatory regime likely will recognize that there is rough parity in the importance of federal interests in protecting UCTI vis-à-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 the final version of SP 800171, the present DFARS may become a subset of or subsumed by the CUI rule.

Some aspects of cyber supply chain requirements will be agency-specific. For example, event response and incident reporting obligations, as follow a cyber breach, could be set by individual agencies.

Measures that protect federal information when in contractor hands also will protect valuable contractor information where the controls are employed across an organization. If the measures contemplated by SP 800-171 are implemented as solicitation requirements and through contract terms, the required controls, like those of the DoD UCTI counterpart, will affect (and likely elevate) the cyber protection practices of thousands of U.S. companies.[29]

SP 800-171, in its abstract, asserts:

> The protection of sensitive unclassified federal information while residing in nonfederal information systems and environments of operation is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations. This publication provides federal agencies with recommended requirements for protecting the confidentiality of Controlled Unclassified Information (CUI) as defined by Executive Order 13556, when such information resides in nonfederal information systems and organizations. The requirements apply to: (i) nonfederal information systems that are beyond the scope of the systems covered by the Federal Information Security Management Act (FISMA); and (ii) all components of nonfederal systems that process, store, or transmit CUI.

Notwithstanding these commendable purposes, objection can be raised as to implementation. SP 800-171 does not resolve *what* constitutes CUI that requires protection.[30] 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 SP 800-171 – and the implementation costs of potentially required controls.

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 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 cyber controls recommended by SP 800-171. The significance of SP 800-171 may not yet have been suitably appreciated by those in the federal supply chain who will be affected by it. SP 800-171, however, explicitly recognizes the federal government's unprecedented reliance upon ''external information system service providers'' (such as contractors). The publication's stated purpose is to:

> ''provide federal agencies with recommended requirements for protecting the *confidentiality* of CUI when such information resides in nonfederal information systems and organizations.''[31]

(Emphasis in original). These ''recommended 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 to 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.[32] Contract clauses can be expected that

[27] The DFARS UCTI rules reference just 51 of the SP 800-53 controls. 78 Fed. Reg. 69281. As proposed in the initial public draft, SP 800-171 specifies 115 controls – the same number as in the SP 800-53 ''Low'' baseline. The Framework lists 124 SP 800-53 controls. The ''Moderate'' baseline of SP 800-53 calls for 221 controls. The ''High'' Baseline references 289 controls.

[28] ''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 p. B-2, is ''[i]nformation that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations and government policies,'' excluding classified information.

[29] The national interest in served if such measures protect against exfiltration of valuable proprietary and enterprise data of private companies in the federal supply chain.

[30] 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/.

[31] SP 800-171, n.6, *supra*, at Section 1.1.

[32] The policy of the federal government is to limit awards to ''responsible'' prospective contractors only. FAR 9.103(a). A

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.[33]

SP 800-171 should be improved so that its purposes can be accomplished effectively and affordably and without foreclosing the government from access to private sector innovation or excluding necessary access to the global supply chain. Potentially affected companies may have cyber measures as good as what SP 800-171 would require, or better. Care is needed to recognize the diversity of contractor circumstances and to credit companies for equivalent cyber protection measures where reflective of recognized standards or practices, even if different than those that SP 800-171 invokes from SP 800-53. Cyber and supply chain security are not and will not become, ''one-size-fits-all'' propositions.[34]

As drafted, SP 800-171 focuses on systems to protect CUI, and presumes that companies potentially subject to CUI security obligations know whether CUI is resident on or transits through their information systems. Unfortunately, this is not the case today. NARA has not finished its work. Indeed, SP 800-171 acknowledges that NARA intends to issue a federal regulation (or directive) to establish the required controls and CUI markings, government-wide. While a proposed rule is said to be under Office of Management and Budget (OMB) coordination, it has not been released for public consideration and comment. Until it is, and 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 controls. Not all information will merit controls and not all controls are merited for all information. Without action of NARA and other federal agencies to answer these crucial questions of scope and definition, the potential use of SP 800-171 to protect federal CUI may prove illusory.

Similarly, SP 800-171 is not now accompanied by specific ''acquisition planning'' or ''contract administration'' measures as will be necessary for agencies to implement the cyber protection measures. The specified controls have little better than abstract significance to private industry or other non-federal actors absent contractual implementation. Until CUI is defined and acquisition mechanisms are in place, neither the government nor industry will know whether or which NIST controls apply or what information is subject to the controls.[35]

Absent from SP 800-171 are specific instructions for reporting of cyber incidents.[36] 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 the private sector.[37] 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.

Nowhere in SP 800-171 is there reference to NIST's *Framework for Improving Critical Infrastructure Cybersecurity*. 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. NIST should consider how it can utilize the Framework for controls and practices that are to be required to protect CUI on nonfederal information systems. 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.''[38] 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

---

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 December 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 here*.

[33] 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.

[34] The Framework rejects a ''one-size-fits-all approach to managing cybersecurity risk for critical infrastructure.'' Framework, at p.2.

[35] 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.

[36] 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.''

[37] Executive Order, ''Promoting Private Sector Cybersecurity Information Sharing,'' Feb. 13, 2015, *available at* http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[38] NIST Framework, n.12, *supra*, at p.2.

  FCR ISSN 0014-9063

guide implementation.[39] This could reduce compliance and implementation burdens on federal contractors.

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.

[39] Articulating the nonfederal information system CUI protection requirements as a Framework ''Profile'' and an implementation ''Tier'' would also facilitate determinations of equivalency between SP 800-53 controls and commercial standards that a nonfederal entity might already have in place. *Id.* at pp. 4-5, 13-14 (the Framework's risk-based approach to managing cybersecurity risk consists of a ''Core,'' ''Profiles,'' and ''Tiers''). The Core of the Framework is not a checklist that companies are required to implement. Instead, the Framework tasks companies to select a Profile and Tier to guide their risk assessments. Core requirements can vary based on the Profiles and Tiers selected. At present, therefore, it is difficult to map compliance between the Framework and SP 800-171.