Preparing for NIST SP 800-171

January 23, 2018
For the American Council of Engineering Companies

Presented by

Jon Williams, Partner
jwilliams@pilieromazza.com
(202) 857-1000

Kimi Murakami, Counsel
kmurakami@pilieromazza.com
(202) 857-1000

© PilieroMazza PLLC 2018

About PilieroMazza

PilieroMazza PLLC is a full-service law firm with offices in Washington, DC and Boulder, CO. We are most well known as a government contracting firm and for 25 years we have helped our clients navigate the complexities of doing business with the federal government. We also provide a full range of legal services including advice on corporate, labor and employment, SBA procurement programs, and litigation matters. Our clients value the diverse array of legal guidance they receive from us and our responsiveness as we guide their growth and secure their success.

Our primary practice areas are:

- Government Contracting
- Small Business Programs
- Labor & Employment
- Business & Corporate
- Litigation

Sign up for our newsletters and blog at
www.pilieromazza.com

© PilieroMazza PLLC 2018

Overview

- What is NIST SP 800-171?
- Who has to comply?
- What to do if you have to comply
- What are the consequences that could arise for noncompliance and how to mitigate those risks
- What is the effect on non-DOD contracts

© PilieroMazza PLLC 2018

What Is NIST SP 800-171?

- Developed by NIST together with National Archives and Records Administration ("NARA")
- Latest version is Revision 1, issued December 2016
  - Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
- Geared specifically toward nonfederal systems to provide standardized security requirements for protecting controlled unclassified information ("CUI")
  - Outgrowth of Congress' direction to NIST in the Federal Information Security Management Act ("FISMA")
  - Security requirements are derived from Federal Information Processing Standards ("FIPS") Publication 200 ("basic security requirements") and NIST Publication SP 800-53 ("derived security requirements")

© PilieroMazza PLLC 2018

What Is NIST SP 800-171?

- Performance-based to avoid mandating specific solutions and to facilitate use of contractor's existing security practices/systems
- Organized into 14 security "families":

Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Management
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

© PilieroMazza PLLC 2018

Compliance with NIST SP 800-171

- Compliance is required under DFARS 252.204-7012
- Deadline for implementation was December 31, 2017
- DFARS 252.204-7012 is not a new requirement, however
  - For all contracts awarded prior to **10/1/17**, contractors should have notified the DoD CIO via email within 30 days of award if the contractor had not implemented requirements in NIST SP 800-171 by the time of contract award

© PilieroMazza PLLC 2018

Who Had to Comply by 12/31/17?

1. Contractors with DoD contracts containing **DFARS 252.204–7012**
   - This DFARS clause should be in all DoD contracts, including commercial item procurements, except for contracts solely for the acquisition of Commercial Off the Shelf ("COTS") items
2. That own or operate a **nonfederal** contractor information system
   - Different security requirements apply to contractor information systems part of an IT service or system operated on behalf of the Government (i.e., a federal system)
3. And have **CUI** in their nonfederal contractor information system

© PilieroMazza PLLC 2018

Drill Down on CUI

- Covered defense information means unclassified controlled technical information or other information as described in the CUI Registry
  - CUI Registry is available at: www.archives.gov/cui/registry/category-list.html
  - The CUI Registry organizes CUI into 25 different industry categories (some with subcategories) such as agriculture, immigration, intelligence, tax, and transportation
- Two key points on CUI:
  - Government must mark or otherwise identify the CUI in the contract, task order, or delivery order and provide it to the contractor in support of contract performance; or
  - The contractor (or another party on its behalf) collects, develops, receives, transmits, uses, or stores CUI in support of the contract

© PilieroMazza PLLC 2018

Real-World Examples of CUI

- CUI is a broad category that can encompass many different types of sensitive, but not classified, information, including:
  - Personally identifiable information such as health records
  - Engineering drawings, plans, designs, blue prints
  - Technical reports and analyses
  - Software code developed under the contract

© PilieroMazza PLLC 2018

Who Is Not Covered (Yet)?

- Contractors that do not perform on DoD contracts containing DFARS 252.204-7012 do not need to comply
  - The clause does not apply retroactively
  - However, a CO could modify your contract to add the clause
- For Non-DoD contractors, NIST SP 800-171 is coming to the FAR (potentially as soon as this year) and could already be required by a civilian agency or contract
  - In the meantime, FAR 52.204-21 (implemented in June 2016) should be in most civilian agency contracts and contains basic safeguarding requirements for contractor information systems based on NIST SP 800-171, but does not explicitly require compliance with NIST SP 800-171

© PilieroMazza PLLC 2018

Exception for COTS

- DFARS 252.204-7012 (and its requirement to comply with NIST SP 800-171) does not apply to contractors that **only** perform contracts that are **solely** for COTS, which are:
  - A commercial item;
  - Sold in substantial quantities in the commercial marketplace; and
  - Offered to the federal government, under a contract or subcontract at any tier, without modification, in the same form as it is sold in the commercial marketplace
- If you have some contracts that are not for COTS, or not solely for COTS, the blanket exception does not apply

© PilieroMazza PLLC 2018

Exception for Commercial Item Contracts?

- Unlike for COTS, there is no blanket exception for commercial items
  - All COTS are commercial items, but all commercial items are not necessarily COTS
- DFARS 252.204-7012 recognizes that, on many commercial item procurements, DoD does not provide covered defense information to the contractor as a necessary component of performing the work
  - In this scenario, DFARS 252.204-7012 (and the requirement to comply with NIST SP 800-171) does not apply

© PilieroMazza PLLC 2018

Applicability to Subcontractors

- DFARS 252.204-7012 (and the requirement to comply with NIST SP 800-171) must be flowed down to subcontractors, **but only** when subcontract performance is for "operationally critical support" or CUI is necessary for performance of the subcontract
  - Operationally critical support is essential to mobilization, deployment, or sustainment of the Armed Forces in a contingency operation
- Contractor may consult with the CO if uncertain about whether to flow down the clause to subcontractors

© PilieroMazza PLLC 2018

Applicability to Small Businesses

- No exceptions for small businesses – if the requirements apply, they apply the same to large and small contractors
- Solicitations should advise when compliance is necessary, which DoD believes gives small businesses time to bring their system into compliance and negotiate the terms of the contract
  - Negotiation may mean submitting a request to be excluded from certain requirements in NIST SP 800-171 or to use alternatives

© PilieroMazza PLLC 2018

Why Compliance is Critical

- Compliance creates a competitive advantage for prime contracts and subcontracts
- Non-compliance could lead to "the parade of horribles"
  - Breach of contract damages
  - Termination for default and reprocurement costs
  - Negative past performance reviews
  - Poor evaluation rating
  - Vulnerability in post-award protests
  - False Claims Act exposure
  - Suspension and/or debarment

© PilieroMazza PLLC 2018

Understand NIST SP 800-171

- Examine the requirements
- Perform a "gap assessment" of your system and practices compared to requirements
- Your current system/practices may not be as far off as you fear
  - Need to determine what your company policy should be and how to configure your system to implement the policy
  - Outside consultants specialize in this assessment if you cannot do it all internally – but no third party "certificate" required for NIST SP 800-171 compliance
- Costs of compliance should be allowable costs

© PilieroMazza PLLC 2018

Utilize NIST Special Publication 800-171A

- Draft of NIST SP 800-171A published last November
- Public comment period closed (after being extended to January 15, 2018)
- This publication is an assessment tool
  - Think of it as a companion guide to NIST SP 800-171
  - Tracks the security requirements within each family
  - Gives questions to be answered to assess whether a company is meeting that security requirement with suggestions
- Available here: https://csrc.nist.gov/publications/detail/sp/800-171a/draft

© PilieroMazza PLLC 2018

Other Resources

- Utilize NIST Handbook 162
  - Provides guidance for assessing IT systems against NIST SP 800-171 geared toward U.S. manufacturers but may be useful for others as well
  - Available here: https://doi.org/10.6028/NIST.HB.162
- Cybersecurity Evaluation Tool ("CSET")
  - Developed by Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT")
  - Step by step process to evaluate IT network security practices
  - Available here: https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

© PilieroMazza PLLC 2018

Put a Security System Plan in Place

- NIST guidance helps you walk through the company policies, processes, and procedures to configure your IT security in order to prepare a System Security Plan
  - At a minimum a "basic" or "simple plan" according to testimony of Ellen Lord, Under Secretary of Defense for Acquisition, Technology, and Logistics speaking before the U.S. Senate, Committee on Armed Services on December 7, 2017
  - DoD may provide a template but it is not available yet
- Develop plans of action for implementation or mitigation if certain requirements have not been met and submit to contracting officer

© PilieroMazza PLLC 2018

Requests for Variance

- Contractors are not expected to follow one defined path, that is why the requirements are performance based
- If you should be excepted from a requirement, or have a suitable alternative, request a variance
- Requests must be submitted in writing to the CO
- For new contracts, DFARS 252.204-7008 indicates a variance should be requested early in the selection process so approval can be included in the contract
- DoD will consider if the alternative is equally effective or if the condition requiring the security control is not present

© PilieroMazza PLLC 2018

Compliance Tips for Small Businesses

- Compliance can be difficult and costly for small businesses, but you may already have systems in place to protect your information that also satisfies NIST SP 800-171, so leverage your existing systems and practices as much as you can
- For companies new to the requirements, DoD suggests a "reasonable approach" provided in FAQ
- Available here: http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf

© PilieroMazza PLLC 2018

DoD's "Reasonable Approach" For Compliance

- Does the company have proper policies or processes?
- Has the IT been configured securely?
- Does the company need security-related software (e.g., anti-virus) or additional hardware (e.g., firewall)?
- Refer to the mapping table in Appendix D to NIST SP 800-171 and check the corresponding security control in NIST SP 800-53
- Can in-house IT personnel accomplish changes or does company need outside assistance?

© PilieroMazza PLLC 2018

Other Applicable Requirements

- If you are subject to DFARS 252.204-7012, be mindful of other requirements you have to meet under the clause beyond NIST SP 800-171, including:
  - Rapid reporting (72 hours) of any cyber incident that affects a covered contractor information system, the covered defense information, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract
  - Preservation and government inspection requirements
  - Reporting on malicious software
  - Ensure cloud service providers, if used, follow certain security requirements

© PilieroMazza PLLC 2018

Tips and Takeaways

- Review your contracts with agencies and third parties
  - Are the cybersecurity FAR or DFARS clauses included, or are any other contract-specific cybersecurity requirements imposed?
  - Did the government mark CUI?
  - Do your contracts with primes, subs, JV partners, etc., include proper flow down clauses and allocation of risk/liability?
- Develop a written plan for implementing necessary security measures
- Perform a technical gap assessment and necessary changes to IT system configuration
- Explore cybersecurity and online property insurance

© PilieroMazza PLLC 2018

Tips and Takeaways

- Prepare and negotiate variance requests
- Draft, revise, and update internal controls, procedures, and policies to ensure compliance with the applicable security requirements
  - Critical to have buy-in at all levels of the organization and clear company policies in support
  - Incorporate into your employee handbook
  - Train your people
  - Spell out processes and chain of command for oversight and responding to a security issue

© PilieroMazza PLLC 2018

Questions?

Jon Williams
jwilliams@pilieromazza.com

Kimi Murakami
kmurakami@pilieromazza.com

PILIERO MAZZA

888 17th Street, NW
11th Floor
Washington, DC 20006
202-857-1000

This material is presented with the understanding that the author is not rendering any legal, accounting, or other professional service or advice. Because of the rapidly changing nature of the law, information contained in this presentation may become outdated. As a result, the user of this material must always research original sources of authority and update information to ensure accuracy when dealing with a specific legal matter. In no event will the author be liable for any damages resulting from the use of this material.

© PilieroMazza PLLC 2018