When you have to be right

The following pages are an excerpt taken from Cybersecurity in the Digital Age: Tools, Techniques, & Best Practices by Gregory A. Garrett

THE TOP SIX CYBERSECURITY PAIN POINTS FOR GOVERNMENT CONTRACTORS

1. How can government contractors accurately and cost effectively assess their cybersecurity compliance to NIST SP 800-171?

First, it is important to understand that NIST SP 800-171 is a set of guidelines established to help companies protect their CUI and DOD covered defense information (CDI) in non-federal systems and organizations. CUI is a result of the Obama Administration Executive Order 13556 issued in November 2010. The CUI system aims to standardize and simplify how the government handles unclassified information that requires safeguarding. There are 22 approved CUI categories of information, covering everything from agriculture, transportation and energy to defense technical drawings and product specifications provided by federal government agencies to government contractors.

Second, according to NIST, there are two classifications of security requirements: basic and derived. The basic security requirements are obtained from the Federal Information Processing Standard 200 (FIPS 200), which provides high-level fundamental security requirements for federal information and information systems. The derived security requirements, which supplement the basic security requirements, are taken from the detailed security controls contained in NIST Special Publication 800-53.

Third, for a government contractor to ensure it receives an accurate and cost-effective assessment of its cybersecurity capabilities in comparison to the NIST SP 800-171 guidelines, it should competitively evaluate and select an independent professional services company with the ability to perform a high-quality and timely cyber risk and gap assessment.

Currently, it appears that many government contractors do view the NIST 800-171 guidelines as a mandatory rule that requires full and strict compliance. It is expected that the new DFARS 252.204-7012 cybersecurity and information security management systems will be treated in the same manner as the six current major contractor business systems: accounting, cost estimating, material management and accounting system (MMAS), government property management and earned value management system (EVMS).

2. What actions have U.S. government contracting officers taken when government contractors have failed to comply with the DFARS 252.204-7012 (NIST SP 800-171 compliance requirement) since the Dec. 31, 2017 deadline?

So far, government contractors have been advised via updates from the DOD chief information officer (CIO) that the Defense Contract Management Agency (DCMA) may request a copy of their system security plan (SSP) for purposes of evaluation for compliance with the NIST SP 800-171 requirements and that the Defense Contract Audit Agency (DCAA) may audit their related information security management systems’ cost.

Concerns to consider:
- Currently, neither the DCAA nor the DCMA have the necessary cybersecurity expertise to assess the contractor’s compliance with the standard. Without certified information system security professionals (CISSPs), certified information technology auditors (CITAs) or the like, they cannot accurately evaluate government contractors’ SSFs to fairly assess their compliance with NIST SP 800-171.
- If the federal government decides to outsource the SSP evaluation to assess compliance with NIST SP 800-171, it is imperative to ensure that the selected companies are free of organizational conflicts of interest (OCI) and personal conflicts of interest (PCI).
- If a government contractor is non-compliant with all or part of NIST SP 800-171, then the government contracting officer will have to decide on a number of actions. He or she can:
  - Withhold contractor payments up to 20 percent;
  - Issue a stop work order;
  - Issue a suspension of work; or
  - Terminate the contract for default.

3. How should government contractors pay for this additional cybersecurity compliance expense?

The DCAA has not yet provided specific guidance on how the new cybersecurity compliance-related expenses will be audited. Nevertheless, these costs will likely be audited in a similar manner to the six existing DFARS contractor business systems. Compliance-related business expenses may be categorized as a direct or indirect cost, depending on the contract requirements and the contractor’s accounting system. Often, these DFARS contractor business system requirements are considered indirect costs. Thus, if these cybersecurity management system-related compliance costs are charged as indirect costs, properly allocated and considered fair and reasonable in both nature and amount, they should be deemed as allowable costs.

4. Do I have to purchase cybersecurity liability insurance?

Currently, the FAR and DFARS do not require government contractors to purchase cybersecurity liability insurance.
Cybersecurity in the Digital Age: Tools, Techniques, & Best Practices
by Gregory A. Garrett

Produced by a team of 14 cybersecurity experts from five countries, *Cybersecurity in the Digital Age* is ideally structured to help everyone—from the novice to the experienced professional—understand and apply both the strategic concepts as well as the tools, tactics, and techniques of cybersecurity.

**Among the vital areas covered by this team of highly regarded experts are:**

- Cybersecurity for the C-suite and Board of Directors
- Cybersecurity risk management framework comparisons
- Cybersecurity identity and access management – tools & techniques
- Vulnerability assessment and penetration testing – tools & best practices
- Monitoring, detection, and response (MDR) – tools & best practices
- Cybersecurity in the financial services industry
- Cybersecurity in the healthcare services industry
- Cybersecurity for public sector and government contractors
- ISO 27001 certification – lessons learned and best practices

**Are you prepared to defend against a cyber attack?**

Based entirely on real-world experience, and intended to empower you with the practical resources you need today, *Cybersecurity in the Digital Age* delivers:

- Process diagrams
- Charts
- Time-saving tables
- Relevant figures
- Lists of key actions and best practices
- And more!

**About the Author**

**Gregory A. Garrett** is the head of U.S. and international Cybersecurity for BDO, supporting over 2,000 Information Technology (IT) and cybersecurity professionals worldwide. With more than 30 years of experience, Gregg is a recognized IT and cybersecurity expert, having managed more than $40 billion of complex, high-tech programs, contracts, and related consulting and professional services for government agencies and Fortune 500 companies across the globe.

An expert in strategic business planning, Gregg has significant experience developing and implementing cyber risk management programs designed to increase profitability and manage cost, risk, and compliance. He has significant experience with agile software development, cloud migration, data analytics, supply chain management, and systems engineering. Gregg is also highly skilled with respect to government contract compliance and management.

He is a respected international IT business consultant, acclaimed expert witness, best-selling author of 22 published books, and a highly-decorated former U.S. Air Force military officer. Gregg is the recipient of numerous national and international business awards for his writing, teaching, consulting, and leadership.