CYBERSECURITY UNDER NEW DOD RULES

Roadmap for Implementing the New DFARS Final Rule on Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013–D018)

CKSS
CKSecurity Solutions

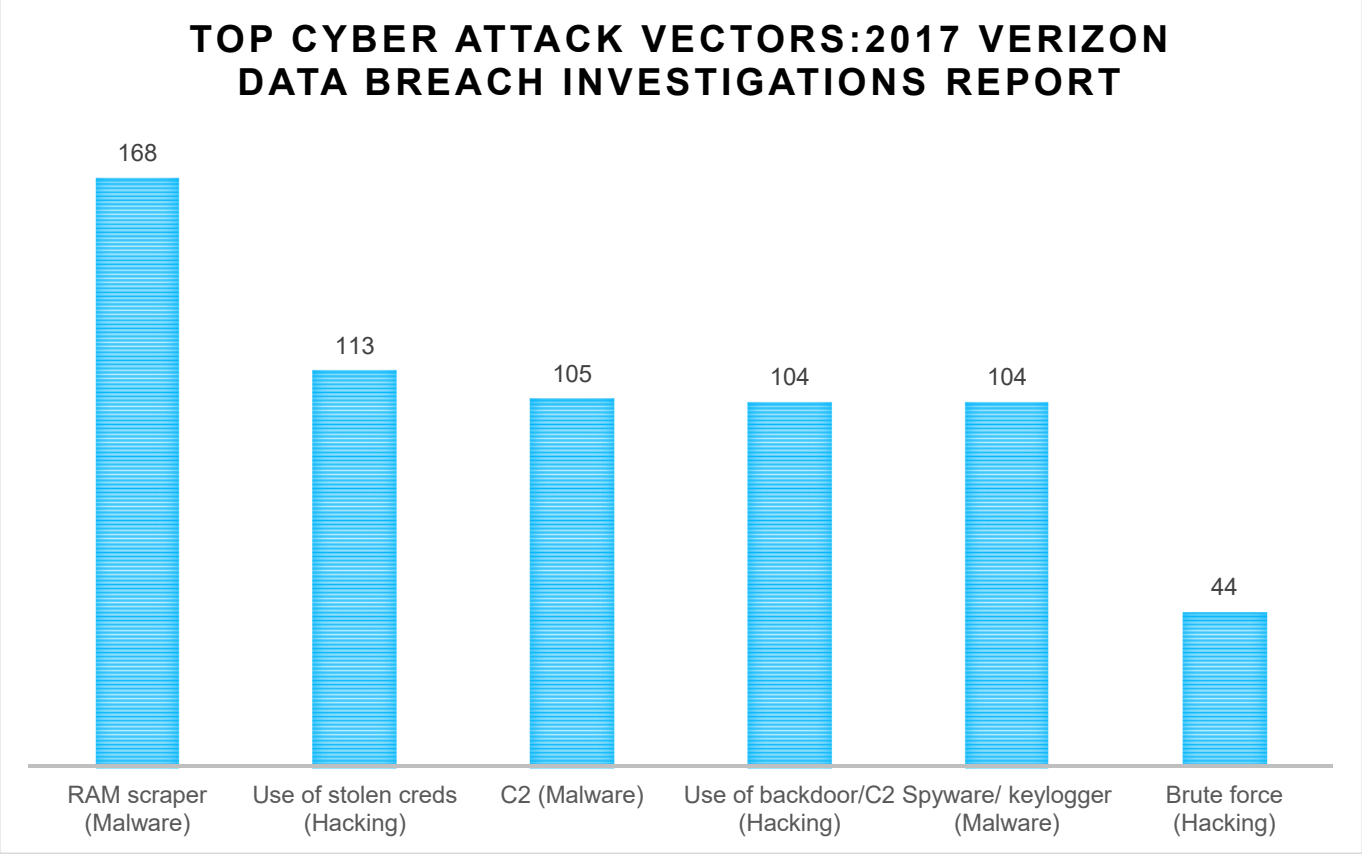
Contents

INTRODUCTION

In response to the recent executive orders and growing pressure from high profile government data breaches, DoD Issued the Final DFARS Rule on Network Penetration and Cloud Computing on October 2016. The final ruling requires covered contractors to implement certain cybersecurity safeguards and report data breaches within 72 hours and adopt NIST SP 800-171 as the baseline for covered information system security requirements.

CONTRACTORS ARE ENCOURAGED TO IMPLEMENT THE ADEQUATE SAFEGUARDING STANDARDS IN NIST SP 800-171 REVIEW 1 AS SOON AS PRACTICAL, BUT NO LATER THAN DECEMBER 31, 2017.

This white paper provides an overview of the new regulatory requirements, definition of Covered Defense Information, DFARS 252.204-7012 Modifications, National Institute of Standards and Technology (NIST) Special Publication (SP) 171, benefits of implementing controls, cost of implementing safeguards, oversight, selecting a cyber security consultant, and a road map to compliance.



OVERVIEW OF REGULATORY REQUIREMENTS

The Final Rule includes the following Provisions and Clauses:

Subpart 204.73	Safeguarding Covered Defense Information and Cyber Incident Reporting
Subpart 239.76	Cloud Computing
252.204-7008	Compliance with Safeguarding Covered Defense Information Controls
252.204-7009	Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting
252.239-7009	Representation of Use of Cloud Computing
252.239-7010	Cloud Computing Services

COVERED DEFENSE INFORMATION

Covered defense information (CDI) is defined as:

- Unclassified controlled technical information or

- Other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html
- That requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—
    - Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of the DoD in support of the performance of the contract; or

    - Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

DFARS 252.204-7012 MODIFICATIONS

WAIVER/DEVIATION REQUESTS FROM NIST SP 800-171 SECURITY CONTROLS

Subcontractors are to notify the prime contractor when submitting such a waiver request; The Contractor shall submit requests to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place." Contractors are required to implement security requirements on all covered contractor information systems supporting the contract performance.

CLOUD SERVICE PROVIDERS (CSPS)

Contractors using cloud computing services during performance of a contract are to ensure that the CSP adheres to the following requirements (i) meet security requirements equivalent to those established by the Government for FedRAMP moderate baseline; and (ii) comply with DFARS 252.204-7012's reporting, protection, and access requirements; and clarify that the clause must be flowed down to subcontractors when CDI is necessary for performance of the subcontract; (iv) and all DOD data is to be maintained within the U.S.

CYBER INCIDENT REPORTING REQUIREMENTS

DOD clarified the definition of a cyber incident as follows: Action taken through the use of computer networks that results in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. Contractors are required to report cyber incidents that affect the contractor's ability to perform contract requirements designated as operationally critical support. Operationally critical support requirements must be marked or otherwise identified in the contract, task order, or delivery order. Within

72 HOURS of discovery, contractors must report a cyber incident to http://dibnet.dod.mil. For at least **90 DAYS** after reporting an incident, contractors are obligated to preserve and protect images of all known affected information and systems in order to allow DoD to determine whether it will conduct a damage assessment. DoD must be given access to any additional information or equipment necessary to conduct a forensic analysis, and any malicious software discovered must be submitted to DoD.

DOD CLASS DEVIATIONS

The contractor will also want to keep in mind the Class Deviation issued by DoD in October 2015. The Class Deviation grants contractors **9 MONTHS** from the date of award to implement derived security requirements 3.5.3 "Use of multifactor authentication" for local and network access to privileged accounts and for network access to non-privileged accounts" under NIST SP 800-171.

NIST SP 800-171

Under DFARS 252.204-7012, a contractor must implement the security requirements in **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION (SP) 800-171**, that is in effect at the time the solicitation is issued by the Contracting Officer, or as soon as practical, **BUT NOT LATER THAN DECEMBER 31, 2017.**

On December 2016, the National Institute for Standards and Technology (NIST) released NIST Special Publication (SP) 800-171 Revision 1. The most notable change involves the addition of a new standard, **PL-2 (SYSTEM SECURITY PLAN),** which is derived from NIST's security and privacy controls standard for federal information systems and organization (SP 800-53). Contractors are to describe in a system security plan (SSP), how the Controlled Unclassified Information (CUI) requirements are met or how organizations plan to meet the requirements. The SSP describes the boundary of the information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems. When requested, the SSP and any associated **PLANS OF ACTION AND MILESTONES (POAM)** for any planned implementations or mitigations should be submitted to the responsible contracting officer to demonstrate the nonfederal organization's implementation or planned implementation of the CUI requirements. In addition, CUI Information will only have only one level of safeguarding (i.e., **MODERATE IMPACT FOR CONFIDENTIALITY**). This means that CUI confidentiality impact value is not lower than Moderate in accordance with Federal Information Processing Standards (FIPS) Publication 199.

Below are the recommended SP 800-171 controls that are required to ensure the confidentiality of CUI:

Three exceptions include:

- **CP-9** *from the contingency planning family;*
- *a requirement to develop and implement a system security plan (derived from* **PL-2***) from the planning family; and*
- *a requirement to implement system security engineering principles (derived from* **SA-8***).*

To ensure that security control deployments provide protection sufficient to address emerging threats, organizations are strongly advised to review the complete listing of SP 800-171 controls and compare it to their individual Security Plans.

CONTRACTORS MUST GO THE EXTRA MILE AND IMPLEMENT NONFEDERAL ORGANIZATION (NFO) CONTROLS. THESE CONTROLS ARE EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.

The government assumes that the contractor has policies, procedures, and security plans in place that are the fundamental building blocks for a mature security program. For example, an incident response plan is required to meet the 72-hour window for reporting cyber Security incidents. However, the incident response plan control (IR-08) is listed as an NFO control.

BENEFITS OF IMPLEMENTING CONTROLS

There are some key value-added benefits of implementing controls.

•Benefit 1

- Implementing the DoD controls can help reduce security risks and mitigate damage if or when incidents occur.

•Benefit 2

- Prevent/protect/mitigate legal damage and costs.

•Benefit 3

- Ensures the viability of on-going contracts, and protects and enhances the reputation and marketability of a contactor.

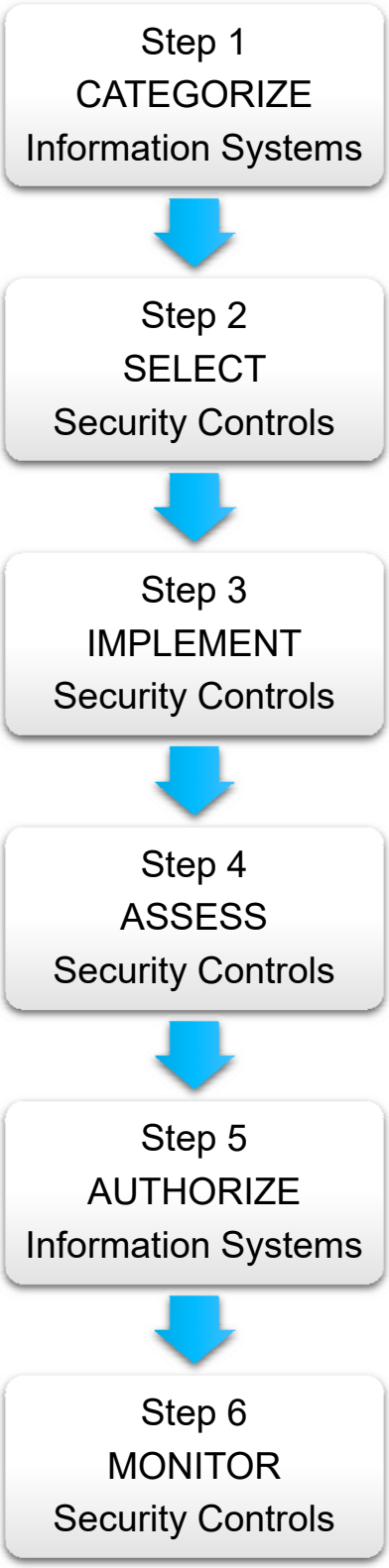
•Benefit 4

- **Differentiator**: The cost savings that comes from avoiding data breaches will vary from one organization to the next. The cost savings will depend on the information assets of the organization, the threats, and vulnerabilities unique to each organization. However, it is a safe assumption that for any contractor who decides that there is an economic benefit to doing business with DoD, implementing safeguards of CDI will be less than the costs that come from a data breach.

•Benefit 5

- **Due Diligence**: Having a robust security program shows commitment to customers, board members, internal groups, auditors, investors, and business partners. Due diligence requires the implementation of a risk management process, with strict controls. NIST 800-37 provides a clear risk management framework needed to ensure security and privacy controls are enacted to protect information systems. The Risk Management methodology ensures a continuous process of checks and balances that should be understood as shown below.

SECURITY LIFE CYCLE



COST OF COMPLIANCE

Meeting the new requirements may initially prove to be costly, especially for small businesses not already equipped with cybersecurity infrastructure. The government does not intend to directly pay for the operating costs associated with the rule.

However, contractors can mitigate the costs of implementing safeguards by spreading fees across multiple contracts, rendering these expenses allowable and chargeable to indirect-cost pools. Other contractors can negotiate higher fees if they only have a few DOD contracts.

OVERSIGHT

The contract administration office is responsible for ensuring that the contractor has a process in place for meeting the required safeguarding standards. In accordance with the terms of the contract, audits or reviews will be conducted at the discretion of the contracting officer. The officer may also request proof of compliance after an incident report.

THE SSP AND POAM DOCUMENTS ARE NOW DELIVERABLES THAT HAVE TO BE SUBMITTED TO THE CONTRACTING OFFICER TO DEMONSTRATE COMPLIANCE.

SELECTING A CYBER CONSULTANT

Effective cybersecurity is much more than checking a box for compliance. The ruling calls for thorough implementation of technologies, processes, and policies. Select a consultant who can provide guidance in choosing appropriate technologies based on best practices, price, and industry feedback. The selected firm should also be able to assist with gap analysis and remediation efforts.

There are a few things to look for when selecting someone to assist with compliance.

- Use LinkedIn to verify employment history and credentials, and remember that a consultant employed by a well-regarded company does not necessarily mean the assigned employee has the relevant experience.
- Explore length of time a company has been providing cyber services; expertise in other areas of compliance does not directly translate into cybersecurity expertise.
- Learn whether or not employees have spoken at security events, written security articles or blogs, and participated in community related security events.
- Also probe to find out more about the type of security employed by the cyber consulting firm in safeguarding your information.

ROADMAP FOR COMPLIANCE

For compliance best practices, contractors should consider the following:

Consult with legal counsel to determine contracts that are subject to the new rule and contractor flow-downs.

Seek accounting advice to capture costs associated with implementing the security safeguards.

Engage the services of an outside provider for advisory services, gap analysis, and implementation of required controls.

Hire an outside consultant to conduct an independent risk assessment and to ultimately validate the various safeguards implemented during the remediation phase.

Conduct continuous monitoring activities.

Contact CKSS for a more detailed approach to compliance.

SOURCES

1. Venable, LLP: The New DFARS Interim Rule on Network Penetration Reporting and Contracting for Cloud Services: Five Immediate Steps Contractors Can Take to Comply.
2. Covington, LLP: New clause DFARS 252.204-7008, “Compliance with Safeguarding Covered Defense Information Controls”.
3. Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (NIST Special Publication 800-171 Revision 1).
4. Arnold & Porter Advisory: NIST Issues Revisions to Special Publication 800-171.
5. Department of Defense-Defense Acquisition Regulations System Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting or Cloud Services (DFARS Case 2013–D018).

ABOUT CKSS

CKSS is a security service provider specializing in Compliance, IT Audits, Advisory Services and Managed Services. Our customers rely on us to improve their Cyber Security Posture.

With years of relevant experience and certifications, CKSS brings a proven approach to cyber solutions across federal, commercial, education, state and local government agencies. CKSS is the best organization for understanding what you need and delivering cost effective, results oriented solutions.

For more information, visit **www.cksecuritysolutions.com.**