QAI SECURITY BRIEF

# CYBER SECURITY FOR FEDERAL CONTRACTORS

Concerns over cybersecurity are rising to the top of the agenda for every government agency. Pressures are increasing on agencies to improve protection of federal information and data. Due to these concerns, agencies are taking initiatives to require contractors to implement cyber safeguards. These new requirements are appearing in solicitations and contracts, and as flow down terms. Companies that want to win contracts need to understand how the federal government expects its contractor's to establish and maintain a cybersecurity posture to defend against and respond to cyber threats.

For companies like Quality Associates, who receive, process and store sensitive customer data, information security is paramount. We focus on every aspect of protecting our clients' material both in its' physical format as well as digital. Attaining and maintaining the levels of security required by our customers is part of doing business and in our opinion is the only way to do business.

The information below will help to explain Controlled Unclassified Information (CUI) – what it is and why it needs to be protected, NIST 800-171 compliance, SPRS Supplier Risk Score attestation and DoDs' CMMC cybersecurity compliance.

QUALITY ASSOCIATES INCORPORATED

A KONICA MINOLTA COMPANY

# CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI is defined as information created by the government, or an entity on behalf of the government, that is unclassified but needs safeguarding. CUI is information that is sensitive and relevant to the interests of the US and potentially it's national security, but is not strictly regulated by the federal government.

Examples of CUI include email, electronic files, blueprints, drawings, proprietary company or contractor information (such as sales orders and contracts), and physical records (such as printouts). It is important to understand that CUI security requirements are not restricted to digital files; CUI can include paper copies, which are specifically referred to as "printed from an information system which processes or stores electronic files transmitted or stored on servers, desktops, laptops, mobile devices, etc."

Let's say that during fulfillment of a federal contract, you receive files or an email with attached files from the agency with which you are doing business. That information (which is CUI) now resides on your company's email system (potentially on that workstation's hard drive) and must be protected. Likewise, if you develop proprietary information for a federal agency or for a prime contractor under a federal contract, that information must be protected. If you receive printouts through the mail or by courier service, that information must be protected.

## NIST SP 800-171 COMPLIANCE

To be eligible to participate in federal contracts, contractors must provide evidence of compliance with NIST 800-171. NIST 800-171 covers the protection of Controlled Unclassified Information (CUI) as defined above.

The NIST security requirements and security controls have been determined over time to provide the necessary protection or federal information and systems which are covered under FISMA (Federal Information Security Modernization Act of 2014). They must be met by anyone who processes, stores, or transmits potentially sensitive information for the Department of Defense (DoD), General Services Administration GSA), NASA, and other federal or state agencies.

## SUPPLIER PERFORMANCE RISK SYSTEM (SPRS)

The Supplier Performance Risk System (SPRS) is a web-enabled enterprise application that gathers, processes, and displays data about supplier performance. It is the DoD's single, authorized application to retrieve supplier performance information.

In 2020, SPRS was updated to document, store, and retrieve Supplier Risk Scores from NIST SP 800-171 Assessments for authorized representatives of the contractor, DoD Components and federal acquisition personnel.

SPRS's Supplier Risk Score provides government procurement specialists with a composite score that considers each supplier's performance in implementation of cybersecurity requirements.


## DoDS' CMMC CYBERSECURITY COMPLIANCE

The Cybersecurity Maturity Model Certification (CMMC) is a unified cybersecurity standard created to increase the security posture of companies operating in government supply chains. By requiring an auditable process under the CMMC, the Department of Defense has mandated measurable cybersecurity standards that must be third-party verified for all contractors.

The Department of Defense has been in the process of gradually migrating from NIST 800-171 to the CMMC framework since January 31, 2021. By October 1, 2025, all new DoD contracts will include CMMC requirements instead of NIST 800-171.

## SOC II TYPE I COMPLIANCE

SOC II Type I is a report on a service organization's system and the suitability of the design of their controls. The report describes the current systems and controls in place and reviews documents around these controls. The design sufficiency of all Administrative, Technical and Logical controls are validated.

## THE BENEFITS OF COMPLYING

The good news for companies that embark on the effort to meet NIST 800-171 or CMMC is that it provides a competitive advantage over companies that have not. Also, a side benefit of becoming compliant with NIST 800-171/CMMC is that once you do, you have also made significant progress on the path to comply with SOC II, another competitive advantage.

Once you meet NIST 800-171/CMMC, you can contact your customers to let them know, and ask them if they know if all their suppliers are compliant.

Even for companies not participating in Federal supply chains, there can be advantages to companies who comply with a cybersecurity framework. Many industries outside of the Federal government will also recognize and reward your compliance with these cybersecurity mandates.

## WHAT IF YOU DON'T COMPLY?

NIST is a non-regulatory agency of the US Department of Commerce. It's not as if auditors will storm your premises to see if you are in compliance. But your contracts will be at risk.

There are ramifications or not being compliant. If an auditor becomes aware that you have not achieved compliance, you can risk losing your existing contracts. If you are a prime contractor, your federal officer could ask you about your plan for compliance with the NIST 800-171 mandate (if they haven't already). If you are a subcontractor, you could be asked by your prime about compliance.

If you don't become compliant with the NIST 800-171 mandate or have a plan in place to do so, you will be ineligible for any potential future contracts.

If a government contractor does not have proof of compliance, the company risks removal from the approved DoD vendor list. The DoD Chief Information officer must now be notified within 30 days of contract award of any security requirements not implemented at the time including cybersecurity compliance.

For contracts with CMMC requirements, you will be unable to participate in the contract unless you meet the CMMC requirements. In other words, you will be ineligible for award of that contract.

There are no fines associated with non-compliance; however, you will be unable to participate in any DoD contracts.

# QUALITY ASSOCIATES IS COMPLIANT WITH THE FOLLOWING (UPDATED 8/24/2022):

Quality Associates' security posture has been assessed and verified by a "CMMC 3rd Party Assessment Organization" or C3PAO with a very high assessment score.

We have achieved the following compliance certifications:

- NIST 800-171 Compliance
- Assessment score of 97 registered in SPRS
- CMMC Level 2 Certification
- SOC II Type I Compliance

QUALITY ASSOCIATES INCORPORATED
A KONICA MINOLTA COMPANY

KONICA MINOLTA

11850 West Market Place, Suite P | Fulton, MD 20759
800.488.3547 **QualityAssociatesInc.com**

GSA Schedule 47QTCA23D000A

GPO MATOC 951-M