SQUIRE PATTON BOGGS

Security Developments for Government Contractors:
Interim Rule on Use of Cloud Services

Government contractors selling to the US Department of Defense (DoD) bidding on future contracts must determine whether they or any subcontractors anticipate using cloud computing services and, if so, must take steps to ensure the security and confidentiality of government information, according to an interim rule issued by DoD August 26, 2015.

Overview of the Interim Rule

DoD issued the interim rule to implement previously issued guidance and policy for the acquisition of cloud computing services. The rule, which largely implements prior DoD guidance, provides standard contract language for the acquisition of cloud computing services, including access, security and reporting requirements.

The interim rule also stipulates that cloud services can only be provided by a cloud service provider (contractor or subcontractor, regardless of tier) that has been granted provisional authorization by Defense Information Systems Agency, at the level appropriate to the requirement, to provide the relevant cloud computing services.

Lastly, the interim rule mandates that cloud computing service providers are required to maintain within the 50 states, the District of Columbia, or outlying areas of the United States, all government data that is not physically located on DoD premises, unless specifically otherwise authorized.

Details of the Interim Rule

The interim rule largely implements the policies and procedures set forth under both:

- Cloud Computing Security Requirements Guide (SRG) Version 1, Release 1 , issued on January 13, 2015, for cloud service providers to comply with when providing the DoD with cloud services (see http://iase.disa.mil/cloud_security/Pages/index.aspx – note that both a draft of Release 2, issued July 24, 2015, and supplemental guidance issued August 7, 2015 and August 27, 2015, are also available at this link).
- The DoD Chief Information Officer's memo of December 15, 2014, titled "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services." (See http://iase.disa.mil/cloud_security/Pages/docs.aspx).

As part of the implementation, the interim rule provides definitions for a number of key terms critical to understanding and complying with its requirements:

- **Cloud computing:** a service model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.
- **Government data:** extremely broadly defined to include any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by the government in the course of official government business.
- **Government-related data:** also broadly defined to include any information, document, media, or machine readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of government data. This does not include a contractor's business records (e.g., financial records, legal records, etc.) or data such as operating procedures, software coding, or algorithms that are not uniquely applied to the government data.
- **Spillage:** a security incident that results in the transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.
- **Authorizing official:** the senior federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation (this is as described in DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," a copy of which is available at https://rmf.org/index.php/what-is-rmf/65-rmf-dod.html).

Specific Requirements of the Interim Rule

Changes to the Defense Acquisition Regulations System (DFARS) as a result of this interim rule include:

- A new provision in DFARS 252.239–7009: Representation of Use of Cloud Computing is added, requiring contractors responding to any solicitation must indicate whether or not they anticipate cloud computing services will be used in the performance of the contract or any subcontract. If the anticipated usage of cloud services is not indicated by a contractor but the contractor subsequently desires to utilize cloud services, then the contractor is required to obtain approval from the contracting officer prior to utilizing cloud computing services in performance of the contract.
- New DFARS 252.239-7010 requires that if cloud services are used, then the contractor must implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing SRG (version in effect at the time the solicitation is issued or as authorized by the contracting officer found at http://iase.disa.mil/cloud_security/Pages/index.aspx).
- DFARS 252.239.7010 also requires that all government data that is not physically located on DoD premises must be maintained within the United States or outlying areas, unless the contractor receives written notification from the contracting officer to use another location.
- Under the interim rule, limitations are imposed on access to, use and disclosure of, government data and government-related data maintained via cloud services. These include requirements to (i) limit access, use, or disclosure of government data strictly to purposes specified in the applicable contract, task order or delivery order, (ii) ensure that contractor employees are subject to all such access, use, and disclosure prohibitions and obligations, and use government-related data only to manage the operational environment that supports the government data, and not for any other purpose. No exceptions to the foregoing are permitted unless specifically authorized. These obligations extend beyond the expiration or termination of the applicable contract.
- Contractors are mandated to report all cyber incidents related to the cloud computing services to the DoD via http://dibnet.dod.mil/. Contractors using cloud services are also subjected to newly issued companion interim cyber incident reporting rules that apply to both cloud computing as well as other information systems cyber incidents.
- DFARS 252.239.710(I) mandates that contractors are required to flow-down the cloud service requirements to all subcontractors if the contract involves or may involve cloud services, including subcontracts for commercial items.

Actions Government Contractors Must Undertake in Order to Comply

- When bidding on future government contracts, whether as a primary contractor or subcontractor, determine if the use of cloud services is anticipated and ensure that the correct representation is made in any response to a solicitation.
- If a contractor will use or provide cloud services that it owns and operates rather than use a subcontractor, then the contractor should seek to become established with provisional authorization and secure listing at http://www.disa.mil/Computing/Cloud-Services/Cloud-Support. If a contractor desires to use a subcontractor to provide cloud services, then ensure that the subcontractor has provisional authorization and is listed at that site.
- Include the mandated contract clause in all future subcontracts where cloud services may be used.
- Ensure that the physical storage location of cloud services is within the United States or outlying areas of the United States.
- Ensure that employees, as well as employees of subcontractors, are aware of and bound by appropriate confidentiality obligations.
- Establish appropriate verification systems and processes to ensure that subcontractors have implemented similar compliance procedures.

Contact

Robert B. Webb III
Partner
T +1 703 720 7855
E robert.webb@squirepb.com

SQUIRE PATTON BOGGS

Security Developments for Government Contractors:
Electronic Parts, Systems and Embedded Software and Firmware

Government contractors selling to the US Department of Defense (DoD) must utilize "trusted suppliers" to obtain and use electronic parts or items that contain electronic parts, according to a rule proposed by DoD September 21. In addition, contractors must maintain "traceability" of any electronic parts from the original manufacturer to the point where the government accepts delivery.

Overview of Proposed Rule

DoD's proposed rule relates to "supply chain risk," and would mandate requirements for secure sources of electronics parts for defense contractors and subcontractors at all tiers. The proposed rule would have a number of ramifications for contractors providing:

- electronic parts
- end items, components, parts, or assemblies containing electronic parts
- services, if the contractor will supply electronic parts or components, parts, or assemblies containing electronic parts as part of the service

The objective of this rule is to protect DoD against risks arising out of the supply chain. The rule represents a supplement to the final Defense Acquisition Regulations System (DFARS) rule on "detection and avoidance of counterfeit electronic parts," which was issued on May 6, 2014.

Key provisions and changes in the proposed rule are:

- Removal of embedded software or firmware from the definition of "electronic part." However, commentary accompanying the proposed rule indicates that DoD expects to address this issue via a subsequent rule.
- Clarification of traceability expectations. The rule proposes definitions of "trusted supplier," "original manufacturer," and "authorized dealer." Contractors and subcontractors that are not the "original manufacturer" would be required to have a risk-based system to trace electronic parts from the original manufacturer to product acceptance by the government, or, if such traceability is not feasible for a particular part, the contractor's system must provide for the consideration of an alternative part or the utilization of tests and inspections in order to avoid counterfeit electronic parts.
- If it is not possible to obtain an electronic part from a trusted supplier, contractors would be required to notify the contracting officer who would then become responsible for inspection, testing, and authentication, in accordance with existing applicable industry standards, of electronic parts obtained from sources other than a trusted supplier.
- The proposed rule would apply to contracts for the acquisition of commercial items, including commercial off the shelf goods, as defined at FAR 2.101.
- Application of the proposed rule would not be limited to contractors subject to cost accounting standards, but would also apply to small business set-asides and would incorporate flow-down to subcontracts, including subcontracts for commercial items, thus applying to all DoD contractors and subcontractors at all tiers that are providing electronic parts or assemblies containing electronic parts.

Details of the Proposed Rule

For purposes of this proposed rule, the following new or amended definitions would be added to the DFARS:

- **Authorized dealer:** a supplier which has a contractual arrangement with the original manufacturer or current design activity, including an authorized aftermarket manufacturer, to buy, stock, repackage, sell, and distribute its product lines. The commentary to the proposed regulation makes express note that "authorized dealer" does not equate to "authorized reseller" since an authorized reseller is not bound to obtain parts from the original manufacturer, but could instead source parts from an authorized dealer, an aftermarket manufacturer, or an independent distributor.
- **Original manufacturer:** includes the "original equipment manufacturer," a "contract electronics manufacturer," and the "original component manufacturer."
- **Original equipment manufacturer:** an organization that manufactures products that it has designed from purchased components and sells those products under the company's brand name.
- **Original component manufacturer:** an organization that designs and/or engineers a part and is pursuing, or has obtained, the intellectual property rights to that part.
- **Contract electronics manufacturer:** a manufacturer that produces goods, using electronic parts, for other companies on a contract basis under the label or brand of the other organizations, or fabricates an electronic part under a contract with, or with the express written authority of, the original component manufacturer, based on the original component manufacturer's designs.
- **Trusted supplier:** includes (i) the original manufacturer, (ii) an authorized dealer for the part, (iii) a supplier that obtains the part exclusively from the original component manufacturer of the part or an authorized dealer, and (iv) a supplier that a contractor or subcontractor has identified as a trustworthy supplier, using DoD-adopted counterfeit prevention industry standards and processes, including testing.

Substantive Requirements of the Proposed Rule

Simply stated, the main substantive requirement under the proposed rule is that contractors must only obtain and use electronic parts, end items, components, parts, or assemblies containing electronic parts that are supplied by "trusted suppliers." This proposed rule will apply both when the contract is one solely for the provision of goods, and when the contract is for services if the contractor will supply electronic parts or components, parts, or assemblies containing electronic parts as part of the service.

A secondary substantive requirement under the Proposed Rule is an obligation to maintain "traceability"– if the contractor is not the original manufacturer of, or authorized dealer for, an electronic part, then the contractor will be required to establish and maintain risk-based processes (taking into consideration the consequences of failure of an electronic part) that enable tracking of electronic parts from the original manufacturer to product acceptance by the government. This rule applies whether the electronic part is supplied as a discrete electronic part or is contained in an assembly. If the contractor cannot establish traceability from the original manufacturer for a specific part, it must complete an evaluation that includes consideration of alternative parts or utilization of tests and inspections commensurate with the risk

The third and final proposed requirement is that the rule will apply to both prime contractors and to subcontractors at all tiers for all DoD procurements. The rule mandates the flow-down of the rule and the required contract clause to all subcontracts (and thus also sub-subcontractors and suppliers).

Actions Government Contractors Must Undertake in Order to Comply

- Identify and inventory all government contracts that involve the provision of covered electronic parts or components, including service contracts that may be subject to the rule.
- Include the mandated contract clause in all future contracts.
- Implement a reasoned process to establish and verify suppliers under covered contracts as "trusted suppliers" – and take steps to replace those that are unable to qualify.
- Establish appropriate verification by subcontractors that they have undertaken similar actions.
- Establish systems and processes to ensure that the "traceability" requirement is maintained.

Contact

Robert B. Webb III
Partner
T +1 703 720 7855
E robert.webb@squirepb.com