



PRIVACY, DATA SECURITY, INFORMATION LAW & GOVERNMENT CONTRACTS UPDATE

**The Privacy, Data Security & Information Law Practice**

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers.

**The Government Contracts Practice**

Sidley's government contracts lawyers represent clients in all areas of U.S. federal, state and local government contracts, including proposal preparation, cost and pricing structures, contract negotiation, compliance with applicable regulatory structures, post-performance issues and related litigation and export controls. We help clients understand the laws governing agency procurement of products and services and, when necessary, we conduct internal investigations and defend against enforcement and qui tam actions or file claims, appeals or protests related to government decisions or activity.

For more information, please contact:

<b>Alan Charles Raul</b>	<b>Joel Singer</b>
+1.202.736.8477	+1.202.736.8563
araul@sidley.com	jsinger@sidley.com

To receive future copies of this and other Sidley Updates via email, please sign up at [www.sidley.com/subscribe](http://www.sidley.com/subscribe)

*Attorney Advertising - For purposes of compliance with New York State Bar rules, our headquarters are Sidley Austin LLP, 787 Seventh Avenue, New York, NY 10019, 212.839.5300 and One South Dearborn, Chicago, IL 60603, 312.853.7000. Prior results do not guarantee a similar outcome.*

**Cyber Attacks, such as "Advanced Persistent Threat," May Trigger New Requirements for Safeguarding Unclassified Defense Department Information and Reporting**

With the growing phenomenon of cyber attacks on defense contractor information systems by hackers or even hostile foreign entities, the Department of Defense ("DOD") has recently published an "Advance notice of proposed rulemaking ("ANPR")" as a preliminary step toward proposed new Defense Acquisition Regulations System ("DFARS") clauses to address "Safeguarding and Cyber Intrusion Reporting of Unclassified DOD Information Within Industry." 75 Fed. Reg. 9563 (Mar. 3, 2010). While Government contractors obtaining or generating classified information have long been subject to detailed and strict rules on safeguarding such information, *see* Federal Acquisition Regulation ("FAR") clause 52.204-2, unclassified Government information even if not cleared for public release, has not been subject to any standard FAR clause regarding data security. The DOD's attention to these cybersecurity developments may also be instructive for companies that serve as government contractors outside the DOD realm, and for companies involved in critical infrastructure sectors of the economy.

We note that numerous defense and other government contractors have reported being subject to persistent cyber intrusion attempts known as "advanced persistent threat" ("APT"). One defense contractor disclosed the following in a recent SEC filing that may be of interest to many companies:

Like many other government contractors, the Company's computer networks are subject to persistent intrusion attempts. The Company employs increasingly sophisticated technologies, operations and employee training in order to thwart such intrusions, but expects this to be a continuing challenge for the industry. When an intrusion is suspected, the Company takes prompt remedial steps and works closely with government authorities and customers to mitigate any adverse impacts. Based on a recent network intrusion, the Company is notifying

This **Sidley Update** has been prepared by Sidley Austin LLP for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.

customers it believes might have been affected and is working to address customer concerns.

The proposed new DOD rules will create two levels of protection under DOD contracts and subcontracts for “DOD Information,” a term defined as any unclassified information that has not been cleared for public release and is either provided by the DOD to the contractor or its subcontractors or is generated by the contractor or its subcontractors in support of a DOD contract. The proposed arrangement distinguishes between two types of DOD Information that will be subject to either basic or enhanced safeguarding standards.

### **Basic Safeguarding Requirements**

Contractors will normally be required to treat DOD Information using “basic safeguarding requirements and procedures,” which mainly require that contractors (1) not process DOD Information on public computers (such as those available for use by the general public in kiosks or hotel business centers) and not post such information to web pages, unless access is controlled by user ID/password or similar methods; (2) transmit electronic information (such as email and text messages) using technology and processes that provide the best level of security and privacy available in the circumstances; (3) transmit voice and fax information only when the sender has a reasonable assurance that access is limited to authorized recipients; (4) protect the information by at least an electronic barrier, such as login and password; and (5) provide protection against computer intrusions that must include, at a minimum, current and regularly updated malware protection (*e.g.*, antivirus and anti-spyware) and prompt application of security-relevant software upgrades, such as patches, service packs and hot fixes.

### **Enhanced Safeguarding Requirements**

Several types of DOD Information will require that contractors apply enhanced safeguarding requirements and procedures. These types of information include:

- (1) Information designated by the DOD as “Critical Program Information” in accordance with DOD Instruction

5200.39, “Critical Program Information Protection Within the Department of Defense.”

- (2) Information subject to export controls under either the International Traffic in Arms Regulations (“ITAR”) or the Export Administration Regulations (“EAR”).
- (3) Information subject to withholding under the Freedom of Information Act (“FOIA”).
- (4) Information that, under existing DOD procedures, bears designations such as “For Official Use Only,” “Sensitive but Unclassified,” or technical data and computer software where distribution is limited under current DOD directives.
- (5) Personally identifiable information, such as that protected under the Privacy Act or the Health Insurance Portability and Accountability Act (“HIPAA”).

The enhanced safeguarding requirements and procedures that contractors should apply to the above types of DOD Information include:

- (1) Encryption of electronic data, whether in storage or in transit, using encryption technology that has been approved by the National Institute of Standards and Technology or the National Security Agency.
- (2) Protecting networks against cyber intrusion using the same Basic Safeguarding measures discussed above, as well as monitoring inbound and outbound network traffic to block unauthorized ingress, egress and exfiltration, by applying technologies such as firewalls and router policies or host-based security services.
- (3) Implementing information security controls in the project, enterprise or company-wide unclassified security program.

### **Cyber Intrusion Reporting and Cooperation with Government Investigation**

In addition to existing reporting requirements under any law or regulation, the enhanced safeguarding requirements include a

new cyber intrusion reporting requirement covering the following events: (1) an advanced persistent cyber intrusion threat; (2) an event involving data exfiltration or manipulation or other loss of any DOD Information resident on or transiting the contractor's unclassified information system; and (3) any other intrusion activities that allow illegitimate access to an unclassified information system on which DOD Information is resident or transmitting.

All reports will have to be submitted to the DOD's Defense Cyber Crime Center ("DC3") within 72 hours of discovery of the intrusion event and include the applicable dates, threat methodology, an account of the actions the adversary may have taken on the victim systems and the information that may have been accessed, the nature of the contractor information system accessed and the potential impact.

In addition, the contractor will be required to immediately conduct a review of the information systems accessed and identify the affected DOD Information, preserve and protect images of the affected systems until DC3 has received these images and completed its analysis, cooperate with DC3 and share files on compromised systems, as required by the Government and permitted by law. A second DOD office, the DOD Damage Assessment Management Office, will then conduct an initial damage assessment and notify the contractor whether it is required to develop additional reports.

The new DFARS rules impose strict limitations on the Government's ability to share attribution information provided through contractor reports, but allow the Government to use and disclose non-attribution information (*e.g.*, information regarding threats, vulnerabilities, incidents or best practices), at its discretion, to assist other parties in protecting information systems.

## Conclusion

Defense contractors, as well as other government contractors and technology companies, should aggressively monitor and protect their computer systems and resources against advanced network intrusion attempts designed to advance foreign intelligence efforts and/or sophisticated efforts to steal intellectual property and trade secrets. The Defense Department is proposing important new contract terms that will likely impose specific new safeguarding and reporting requirements. Technology companies in other industries should also take note of these significant new developments.

**If you have questions about any of these items, please contact your regular Sidley Austin LLP contact.**

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

**[www.sidley.com](http://www.sidley.com)**

*Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm's offices other than Chicago, London, Hong Kong, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley, or the firm.*

