Westlaw Journal
GOVERNMENT CONTRACT
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 30, ISSUE 5 / JULY 5, 2016

EXPERT ANALYSIS

Privacy and Cybersecurity — Extending the Cybersecurity Defense

By Evan Wolff, Esq., Harvey Rishikof, Esq., and Frederik Van Remoortel, Esq.
Crowell & Moring

Faced with growing cybersecurity threats, federal agencies are rethinking regulations to strengthen networks in both the government and private sectors.

A key effort on this front is the Department of Defense's (DOD) Defense Federal Acquisition Regulation Supplement (DFARS) Safeguarding Rule, which applies to defense contractors. The rule requires contractors to implement dozens of specific security controls in information systems that contain unclassified controlled technical information (UCTI), generally defined as scientific or technical data related to space or military uses. It also requires contractors to notify the DOD if those systems are compromised to the extent that the UCTI could be affected.

The Safeguarding Rule's mandates are to be included in all department solicitations and contracts, including those covering commercial items. But that has not been the case. The rule has been in effect since late 2013, but implementation in DOD contracts has been inconsistent.

However, in February 2015, the DOD criticized its component organizations for not adequately incorporating the rule into their contracts. That was a clear reminder that this is mandatory.

Those mandatory requirements became more complex in August 2015, when the DOD released a revised version of the Safeguarding Rule. The new version requires contractors to implement an expanded set of security controls. And those controls are now mandatory on information systems containing not just UCTI but also other forms of "covered defense information," such as information critical to operational security.

This — combined with the DOD's February statements — suggests that the defense industry will be keeping a close eye on contractor compliance. Companies are likely to see an increased number of federal contract modifications to include the rule after the fact, as well as tighter enforcement of the rule by the DOD.

Contractors working with non-defense agencies will soon be facing similar requirements. Many federal agencies are considering cyber regulations related to procurement. For its part, the Office of Management and Budget (OMB) recently proposed cybersecurity guidelines — similar to the DOD rule — that would apply to all federal contractors. The OMB would like these guidelines to be incorporated into the Federal Acquisition Regulation and adopted by the General Services Administration and other agencies.

The impact of evolving cybersecurity regulations is also beginning to reach corporations well beyond the government contracting sphere. A wide variety of agencies across the federal government, including DOJ, FTC, FCC, SEC, and DHS, are using their current regulatory authority or seeking additional authority to regulate cybersecurity activities in the private sector at large.

The growing focus on cybersecurity creates challenges for companies, but some regulations are making it easier to secure private sector systems. The DHS Support Anti-Terrorism by Fostering

FEDERAL AGENCY LEGISLATION AND OTHER CYBERSECURITY GUIDELINES

The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984	All federal agencies
The Electronic Communications Privacy Act of 1986	All federal agencies
The Computer Security Act of 1987	NIST
The Cyber Security Research and Development Act (November 2002)	NIST, NSF
The Federal Information Security Management Act of 2002 and Federal Information Security Modernization Act of 2014	NIST, OMB, DHS
The Clinger-Cohen Act of 1996	Commerce
The Homeland Security Act of 2002	DHS
DFARS Parts 202, 204, 212, 239, and 252 (August 2015)	DOD
Cybersecurity Guidance Update (April 2015)	SEC
FTC Act Section 5—Data Security Enforcement Actions	FTC
Cybersecurity Unit Best Practices (April 2015)	DOJ
NIST Cybersecurity Framework (February 2014)	All federal agencies
Gramm-Leach-Bliley Act (November 2009)	Multiple federal agencies

Glossary: NIST (National Institute of Standards & Technology), NSF, (National Science Foundation), OMB (Office of Management and Budget), DHS (Department of Homeland Security), DOD (Department of Defense), SEC (Securities and Exchange Commission), FTC (Federal Trade Commission), DOJ (Department of Justice)

Effective Technologies (SAFETY) Act program, for example, limits tort liability arising out of acts of terrorism when companies have implemented DHS-approved security technology.

Enacted as part of the Homeland Security Act of 2002, the SAFETY Act has been applied to physical security-related technologies, such as scanners and metal detectors.

But in 2015, DHS began including cybersecurity technologies in the program, with the approval in April 2015 of cyber-threat detection technologies from the Fire Eye company. That approval is likely to encourage other technology companies to seek approval for their cybersecurity tools as well. And because the liability protections flow up and down the chain, it may motivate companies to purchase and use the approved technologies.

Overall, the federal government's broadening view of cybersecurity is based on the fundamental recognition that national security information isn't just held in places like the CIA or the military. Today, it's also at agencies like the Patent Office or the FDA, as well as in the private sector, with companies on the front line. As a result, federal agencies are realizing that not only are their systems at risk, they also need to focus on their supply chain.

With this growing scrutiny on the private sector, the general counsel now needs to be a critical advisor to the CEO about how to approach the cybersecurity issue and in taking up the issue with the board to allow for proper oversight.

The general counsel needs to make sure the company is seeing this not just as an IT risk but as an enterprise risk that needs to be managed through an appropriate governance structure.



Evan D. Wolff (L) is a partner in **Crowell & Moring**'s Washington office, where he helps lead the privacy and cybersecurity practice. His practice focuses on homeland security, privacy and data security including chemical security regulatory compliance, SAFETY Act, corporate internal investigations, corporate compliance and governance, congressional investigations, cybersecurity and environmental audits. **Harvey Rishikof** (C) is a senior counsel in Crowell & Moring's privacy and cybersecurity and government contracts groups in Washington. His practice focuses on national security, cybersecurity, government contracts, civil and military courts, terrorism, international law, civil liberties, and the U.S. Constitution. **Frederik Van Remoortel** (R) is a senior counsel in Crowell & Moring's Brussels office, where he focuses on corporate, commercial, and labor and employment law. He also advises clients on Belgian and EU data protection and privacy legislation, an area of law that is gaining more and more significance for domestic and international clients. This expert analysis was first published on Crowell & Moring's website. Reprinted with permission.