Published by *Government Contracts Law360* on July 18, 2014. Also ran in *Aerospace & Defense Law360* and *Privacy Law360*.

Notable New Breach Controls For Intelligence Contractors

--By Charles A. Blanchard, Ronald D. Lee, Jeffrey H. Smith and Tom McSorley, Arnold & Porter LLP

Law360, New York (July 18, 2014, 5:39 PM ET) -- Congress has placed significant new network and system security requirements upon federal intelligence community (IC) contractors with the passage of the 2014 Intelligence Authorization Act.[1] The act imposes new requirements for internal controls, security planning and breach disclosure. Contractors must be aware of these new requirements as they are implemented through regulation.

First, the act requires that the Director of National Intelligence (DNI) develop procedures for the reporting by contractors of any "penetration" of IC networks or information systems. Second, the act mandates that, going forward, all IC contracts and contract renewals contain a clause requiring the development and operation of a network and information security plan by each cleared contractor with access to classified information.

These requirements parallel similar regulations the Department of Defense is developing for DOD contractors.[2] Previous DOD regulations regarding the security of networks that process unclassified controlled technical information raised several challenging implementation issues, most notably in their vague definition of what constitutes "adequate" cybersecurity measures.[3] For the IC community, however, such regulations have yet to be written. Thus, IC contractors will have an opportunity to offer comments on any DNI proposal and may be able to help construct clearer, more concrete standards than those offered by DOD thus far.

Cyberincident Reporting

Section 325 of the Intelligence Authorization Act requires each cleared IC contractor, under procedures to be established by DNI, "to rapidly report to an element of the intelligence community ... each successful penetration of the network or information systems of such contractor" that meet criteria established under the new procedures. A "covered network" under this rule is any "network or information system of a cleared intelligence contractor that contains or processes information created by or for an element of the intelligence community with respect to which such contractor is required to apply enhanced protection." The statute does not define what "system penetrations" must be reported, but the act's description of what must be reported offers some guidance. The act requires that each penetration report must contain: (1) a description of the method or technique used in the penetration; (2) a sample of the malicious software, if it is discovered; and (3) a summary of any information that has potentially been compromised.

The provision also requires that the DNI establish mechanisms by which IC personnel can obtain access to contractor equipment or information to conduct a forensic analysis. In an apparent attempt to limit exposure of the contractor's proprietary information, however, the contractor must only provide access for the purposes of "determin[ing] whether information created by or for an element of the intelligence community in connection with any intelligence community program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated." The access provision requires that the DNI procedures provide for the protection of trade secrets, commercial and financial information, and personally identifying information. The procedures also must prohibit the dissemination of information obtained in the course of responding to any cyberincident

outside of the intelligence community, except with the approval of the contractor, or to specific congressional committees, or to law enforcement in connection with the investigation of a specific breach.

Network and Information Security Planning

In addition to the disclosure procedures, Section 502 of the Act requires that DNI, in consultation with the elements of the intelligence community, ensure that any contractor with access to "a classified network or classified information" develop and operate a security plan. The provision does not offer any substantive requirements for such a plan, but only requires that DNI establish security planning standards "for intelligence community networks." The provision does, however, require that "insider threat detection capabilities and insider threat policies of the [IC] apply to facilities of contractors with access to a classified network." Once established, the act also requires that DNI conduct periodic assessments of each security plan to ensure they comply with the relevant standards. The security planning requirement is prospective — it affects only future contracts or contract renewals entered into after enactment. But, going forward, any IC contract or contract renewal must contain a provision requiring that the contractor comply with DNI's security and planning standards.

DNI Development of Procedures and Standards Under the Act

Overall, the procedures and requirements contemplated by the act contain little detail. Most of the work is yet to be done. DNI now must craft both the cyberincident reporting procedures and the security planning standards contemplated by the act. The reporting procedures must be established by DNI within 90 days after enactment (by the first week in October). However, DNI will not necessarily be starting from a blank slate. The act recognizes that Section 941 of the 2013 National Defense Authorization Act contained a similar requirement for DOD contractors. The rule implementing that requirement is due on Aug. 13, 2014.[4] The Intelligence Act requires that, within 180 days after enactment, DOD and DNI, together, establish procedures by which a cleared IC contractor and cleared DOD contractor may submit a single report to satisfy both reporting requirements.

The 2014 Intelligence Authorization Act does not otherwise require coordination between DNI and DOD. Accordingly, DNI's proposed security standards for intelligence community networks and for contractor planning and operations need not parallel any security standards offered by DOD, or any other agency. Furthermore, IC contractors will have an opportunity, pursuant to DNI's administrative process, to comment on any proposed standards.

[1] See Pub. L. No. 113-126.
[2] See Case No. 2013-D018 (implementation of Section 941 of the NDAA for FY 2013), DFARS Open Cases Report at 8 (July 11, 2014), available at http://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf.
[3] See Charles Blanchard, Ronald Lee, and Nicholas Townsend, "A Closer Look at the Department of Defense's Cybersecurity Rule on Adequate Security and Cyber Incident Reporting," Bloomberg BNA's Privacy and Security Law Report (March 17, 2014), http://www.arnoldporter.com/public_document.cfm?u=ACloserLookattheDepartmentofDefensesCybersecurityRuleonAdequateSecurityandCyberIncidentReporting&id=23514&key=28E2; See also Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039), 78 Fed. Reg. 69,273 (Nov. 18, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27313.pdf (implementing DoD rule on network security for "unclassified controlled technical information").
[4] See DFARS Open Cases Report at 8 (July 11, 2014).

Charles Blanchard is a partner in Arnold & Porter's Washington, D.C., office and former general counsel and chief ethics officer for the U.S. Air Force.

Ronald Lee is a partner in Arnold & Porter's Washington office, former general counsel of the National Security Agency, and former chief of staff of the Central Intelligence Agency.

Jeffrey Smith is senior counsel in Arnold & Porter's Washington office and heads the firm's national and homeland security practice. He is a former general counsel of the CIA, former chief of the Clinton Transition Team at the U.S. Department of Defense, and currently serves on the DOD Legal Policy Advisory Board.

Tom McSorley is an associate in Washington, where his practice focuses on the intersection of law and technology. His practice spans government contracts, national and homeland security, intellectual property and telecommunications.