Published on *The National Law Review* https://natlawreview.com

Extending Cybersecurity Breach Notice Requirements to Intelligence Community Contractors

Article By:

David N. Fagan

As an indicator of the continuing focus of government authorities on **cybersecurity breaches** and potential notification requirements, certain contractors for the federal government may soon face new rapid reporting requirements for successful network penetrations. Specifically, **President Obama** signed the 2014 Intelligence Authorization Act ("2014 IAA") into law on July 7, 2014, starting a 90-day clock under Section 325 of the Act for the Director of National Intelligence ("DNI") to promulgate regulations for "cleared intelligence contractors" to report the successful penetration of their networks and information systems.

Section 325 defines a cleared intelligence community ("IC") contractor as "a private entity granted clearance . . . to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of [the IC]." The new regulations will apply to "covered" networks and information systems that "contain[] or process[] information created by or for an element of the [IC] with respect to which such contractor is required to apply enhanced protection."

The Forthcoming Regulations

The regulations proposed by the DNI will require cleared IC contractors to report the following information to a designated IC element following a "successful penetration" of the contractor's covered network or information system:

- A description of the technique or method used in such penetration;
- A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration; and
- A summary of information created by or for an element of the IC that has been potentially compromised as a result of such penetration.

Section 325 does not specify how quickly the cleared IC contractors will need to report this information, leaving this to the regulators to promulgate. As discussed below, the Department of Defense ("DOD") has already imposed a 72-hour reporting requirement in similar regulations.

IC Access to Covered Networks and Information Systems

In addition to setting forth rapid reporting requirements, the new regulations require IC contractors to allow IC personnel access to their "equipment or information" when there has been a "successful penetration" of covered networks. What constitutes a successful penetration is not defined in the statute. However, it may be telling that the statute provides that access is required so that the IC personnel can conduct a forensic analysis of the penetration to "determine 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." Section 325 also requires that new regulations provide for the "reasonable protection of trade secrets, commercial or financial information" and prohibit the dissemination of information obtained by a forensic analysis outside of the IC without the consent of the contractor. Despite this prohibition on dissemination, Section 325 does not address whether the IC can use the information obtained during its forensic analysis to exclude IC contractors from the supply chain, or to make a responsibility or past performance determination.

Relationship to Other Cybersecurity Requirements

Section 325 is almost identical to Section 941 of the National Defense Authorization Act for Fiscal Year 2013("NDAA 2013"). Section 941 similarly requires the Secretary of Defense to promulgate rapid reporting requirements following the successful penetration of covered networks and information systems. Section 325 attempts to harmonize these section by including a provision requiring the DNI and the Secretary of Defense to jointly establish procedures to allow contractors cleared by both the IC and DOD to submit a single report following a successful network penetration.

The rapid reporting requirements of Section 941 also contained a 90-day clock following the enactment of NDAA 2013; however, that rulemaking has been delayed, with the ad hoc committee's report deadline currently extended to August 13, 2014. If DOD meets this new deadline, DOD's rulemaking may influence the IC's approach.

The new regulations envisioned by Section 325 (and Section 941) also may draw comparisons to the recent DFARS rule for safeguarding unclassified controlled technical information ("UCTI"). The UCTI rule mandates that DOD contractors report cyber incidents, including unauthorized access to information, inadvertent release of information, and/or any other loss or compromise, within 72 hours of discovery. In some ways, the UCTI rule appears broader than the regulations contemplated by Section 325. For example, the UCTI rule applies to all information systems on which UCTI *may* be "resident on" or "transiting through," while Sections 325 (IC) and 941 (DOD) will apply to networks or information systems that "contain or possess" covered information. Additionally, the UCTI rule requires contractors to report more detailed information about the compromise than what is listed in Sections 325 and 941. Given that the UCTI rule is broader, contractors currently in compliance with the UCTI rule may have a head start on complying with the forthcoming IC and DOD regulations.

National Law Review, Volume IV, Number 205