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

Cyber-Breach & NISPOM Conforming Change 2 – It's What's on the Inside That Counts (National Industrial Security Program Operating Manual)

Article By:

Alexander W. Major

Most companies are worried about external threats – things that are coming at their people, their group, their company, their government, **all from an outside actor**. Like government's with an eye on counter-intelligence, however, savvy businesses also realize that their employees can also pose a very real, internal threat. While an insider breach is not necessarily a common event, when it does happen, it tends to happen on a large scale. Last year, the FBI reported that when a malicious insider breach surfaced, it cost industry $412,000 per incident, on average. Over ten years, the average loss per industry is $15 million. And, unless you've been hiding under a rock, you know that the Government is not immune to insider breaches and the reputational impact to federal contractors resulting therefrom. Exacerbating, or perhaps facilitating, this threat is the manner in which companies (and governments) store, transfer, and maintain vital company records and data. With the right password and a $16 thumb drive, an intern can steal the corporate keys to the kingdom, and still be home in time for lunch. Simply put, all employers face the risk of insider threats which are more perilous than ever in the computer age. Recognizing that internal threats are real, the issue, then, is how to stop these threats from manifesting. Learning from recent high-profile mistakes, the Government is trying to make sure its contractors stay ahead of the risk of an internal breach.

In October 2011, the President signed Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, followed, a year later, by a Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*. These directives mandate insider threat programs in federal agencies that handle classified information. They also provide guidance for insider threat mitigation programs premised on "responsible sharing and safeguarding of classified data," with guidelines for programs that will "deter, detect, and mitigate actions by employees who may represent a threat to national security."

Although not the first attempt to address insider threats, the Department of Defense implemented the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* via directive (DoD D 5205.16) on September 30, 2014. In light of recent cause celebre breaches, the directive extends to "contractors and other non-DoD entities that have authorized access to DoD resources as required." The Policy tasks the Under Secretary for Acquisition, Technology and Logistics ("AT&L") to develop policy, or amend the DFARS, "to ensure DoD contracts impose

uniform insider threat program requirements." No additional guidance has been provided as to what those policies or amendments may look like. But, further guidance is waiting in the wings – in the form of "NISPOM Conforming Change 2."

The National Industrial Security Program Operating Manual, or NISPOM, provides the baseline standards for protection of classified information released or disclosed in connection with classified contracts under the National Industrial Security Program. In March 2014, the DoD announced that following the 2013 update to the NISPOM ("Conforming Change 1"), a second update will be forthcoming, "Conforming Change 2." DoD also advised that Conforming Change 2 would incorporate the President's minimum standards for insider threat and cyber intrusion reporting and provide contractors no more than six months to implement the requirements.

Conforming Change 2 is expected to be released sometime in early 2015. Therefore, federal contractors operating within or around the intelligence community would be wise to read and heed the *National Insider Threat Policy Minimum Standards* so as to begin examining/drafting/implementing what will be a mandatory "Insider Threat Program." To stay ahead of things (and make the most of the inevitable short timetable), the standards suggest the following baseline needs:

1. Designation of an Insider Threat Program Manager (a U.S. citizen with appropriate clearance).

2. Be prepared to provide HR and network data records pertinent to insider threats (e.g. personnel files, security files, polygraph examinations and disciplinary files)

3. Conduct insider threat training within 30 days of hiring that includes:

a. The importance of detecting and reporting insider threats;

b. Counterintelligence and security fundamentals such as applicable legal issues;

c. Procedures for conducting insider threat response actions;

d. Laws and regulations on gathering, integration, retention, safeguarding and use of records and data, and the consequences of misuse of such information; and

e. Legal, civil liberties and privacy policies.

4. Conduct monitoring of user activity on classified networks that is:

a. Intended to detect activity indicative of insider threat behavior;

b. In accordance with guidance issued by the Cognizant Security Agency ("CSA"), including the tools or capabilities required by the CSA; and

c. Adherent to federal systems requirements as specified by FISMA, NIST, CNSS and others.

While the implementation of an Insider Threat Program on the human-side of things may be set up with little fanfare, the information assurance requirements may throw many-a-contractor for a loop and should be addressed sooner rather than later. When addressing insider threats there needs to be a significant shift in IT priorities: a company must address data security versus the system/network

security of the past – contractors will need to assess the stores and keep of the castle, not just its walls and moat. And, do not expect NISPOM's Conforming Change 2 to provide any sort of road map describing exactly how a contractor should monitor its classified data. That double-edge sword will belong wholly to the contractor.

When examining data security efforts, a key thing to know is that the "requirements" of FISMA, NIST, and others standards serve only as a starting point upon which contractors must build their secure data solutions; standing alone, they will not – and will never be – sufficient. On the upside, this freedom allows contractors the flexibility to set up systems that better align with their own internal infrastructure. But, on the downside, there is no assurance that a contractor's chosen methods and efforts will be deemed "sufficient" (particularly when any breach will be subjected to merciless second-guessing coming from critics world-wide). This recognition isn't intended to invoke the threat of a looming cyber-auditor boogeyman. Rather, it is attempting to demonstrate yet one more example that cybersecurity cannot be addressed with a simple "check the box" mentality. Contractors, like all commercial companies, must create and invest in a strong, but malleable, data security infrastructure that aligns with the contractor's business needs, recognizes the threats facing the contractor (inside and out, criminal and regulatory), monitor those threats, respond accordingly when those threats are present, and be agile enough when those threats morph. This is not an easy sell to the "C-suite" – it does not come cheap, it does not result in a profit, and, at best, when data security efforts work perfectly, it results simply in business as usual.

Government regulatory efforts, like those to be found in Conforming Change 2, are reinforcing the modern business truth that cybersecurity costs are required despite the fact that the perpetual investments are, in their best light, simple loss prevention measures versus revenue generators. While this hopeless pragmatism will never be expressly stated on the face of any legislation, executive order, or judicial opinion, it can obviously be seen between the lines and in the gaps where no clear standards exist. And, as our parents taught us, it really is what's on the inside that counts – whether it's the Government's intentions or your own cybersecurity infrastructure.

National Law Review, Volume IV, Number 326