Bloomberg Government

Federal Contracts Report™

VOL. 109, NO. 12 MARCH 27, 2018

Cybersecurity for Defense Manufacturing: New Threats Demand Heightened Response

Cybersecurity

Defense industry factories now are targets for cyber-attacks, author Robert Metzger of Rogers Joseph O'Donnell writes. Through network-delivered or supply-chain attacks, adversaries can steal sensitive information and IP, cripple production, degrade product functionality or even destroy defense manufacturing assets. Factory security is vital to our national security and economic well-being. Yet, not enough is being done by the federal government to assure cybersecurity for defense manufacturing. Metzger details steps DoD should take and urges manufacturers to plan for response and recovery in the event of an attack.

BY ROBERT S. METZGER

The *New York Times* reported on March 15, 2018, that the Trump Administration accused Russia of cyber-attacks that targeted and could have shut off nuclear power plants and water and electric systems. Another *Times* story, also dated March 15, 2018, described a ''new kind of cyberassault,'' upon petrochemical facilities in Saudi Arabia. The story described the attack as ''not designed to simply destroy data or shut down the plant.'' Instead, the attack was ''meant to sabotage the firm's operations and trigger an explosion.''

Actually, the threat is not really new, though the publicity given to the attacks was unusual, as was the attribution to Russia as the party responsible for attacks on U.S. infrastructure.

Robert S. Metzger *is an attorney in private practice who heads the Washington Office of Rogers Joseph O'Donnell, a firm that has specialized in public procurement matters for more than 35 years. He served as a Special Government Employee on the Cyber/Supply Chain Task Force of the Defense Science Board. The views expressed herein are personal to Mr. Metzger and should not be attributed the Defense Science Board, to any client of Mr. Metzger or his firm or to any organization with which he is or has been affiliated.*

Exposure extends to factories used for defense manufacturing. A ''cyber/physical'' attack can degrade, disable or even destroy key assets of our manufacturers. Attacks can be targeted at the industrial control systems (ICS), supervisorial control and data systems (SCADA), programmable logic controllers (PLCs) or man-machine interfaces (MMIs) that modern factories depend upon. The impact may be obvious, where an attack halts production. The impact can produce physical damage, as illustrated by the Stuxnet attack that caused Iranian nuclear centrifuges to self-destruct. Or the impact may be insidious. Manufacturing attacks can result in fabrication that is out of tolerance or changes to performance characteristics essential for use in mission environments.

The defense industrial base (DIB) is a target for such attacks. Hostile nation-states have designs to compromise U.S. manufacturing capabilities and very sophisticated capabilities to achieve just that result. Such attacks inflict serious commercial injury, but also can advance nation-state objectives at the expense of our national security.

DoD's Current Cyber Protection Measures

Many who read this will be well aware of the DoD cyber contract clause, DFARS 252.204-7012, by which DoD seeks to better protect ''Controlled Technical Information'' (CTI) and other forms of government Con-

 ISSN 0014-9063

trolled Unclassified Information (CUI) against industrial espionage or other unauthorized access. Does this ''cyber DFARS'' protect defense manufacturers against cyber-physical threats? Unfortunately, the answer is ''no.''

The purpose of the ''cyber DFARS'' is to protect information and information systems. It was never intended to protect physical assets, such as factories and manufacturing equipment. The fundamental obligation imposed by the DFARS is to provide ''adequate security on all covered contractor *information systems*.'' DFARS 204.252-7012 (b) (emphasis added). Threats to operations technology (OT) are not the same as threats to information technology (IT), and methods to protect OT systems – such as ICS, SCADA, PLI, MMI, and so forth – differ from protection of information on IT systems.

There are three ''pillars'' to the present federal effort to protect information and information systems of government contractors.

(1) The **information to be controlled** corresponds to the 23 categories and 84 subcategories of ''Controlled Unclassified Information'' established by rule issued on Aug. 14, 2016, by the National Archives and Records Administration (NARA). One of the CUI categories, ''Controlled Technical Information'' (CTI), is information of military or space application. CUI does not include what private companies create or use in software, firmware or other instructions that run OT systems.

(2) The **safeguards to protect** CUI are established by NIST Special Publication (SP) 800-171, the purpose of which is described as the ''protection of unclassified *federal* information in nonfederal systems and organizations.'' (Emphasis added.) Where companies own ICS, SCADA, PLI or similar data, it is not ''federal information.'' SP 800-171 does not address directly threats to ''integrity'' or ''availability'' of data and code upon which defense manufacturing relies. SP 800-171 presents 110 safeguards, intended to protect CUI, but they have limited benefit to the OT critical to defense manufacturing.

(3) Through the use of **acquisition measures**, such as regulations and contract clauses, notably DFARS 202.252-7012, DoD requires contractors (and their supply chain) to provide ''adequate security'' for ''Covered Defense Information'' (CDI) which includes CTI and other CUI categories. Guidance issued on Sep. 19, 2017, by the Director, Defense Pricing/Defense Procurement (DPAP) establishes that ''[t]he Department must mark, or otherwise identify in the contract, any covered defense information.''

Civilian agencies are working on a counterpart FAR clause to the ''cyber DFARS'' to extend the SP 800-171 protections to CUI that is provided or made accessible to contractors, state and local governments, educational institutions, and other nonfederal entities. Like the ''cyber DFARS,'' if any protection is realized to manufacturing, it will be largely unintended.

What is more, SP 800-171 does not distinguish among programs or products, or categories of information, where the actual impact of compromise is greater than the ''moderate'' impact premise. For some information and information systems, and for some manufacturing systems, the ''impact'' of lost confidentiality, availability or integrity may be *very* high, thus meriting more protection than likely to be achieved by SP 800-171 alone.

The federal government does have other tools to protect defense manufacturing if it so chooses. NIST SP 800-53 (rev. 5 is pending) has many more controls, together with enhancements and instructions, that are relevant to protection of OT. Separately, NIST has released SP 800-82, revision 2 (''Guide to Industrial Control Systems (ICS) Security''), which specifically addresses OT systems and informs users how to apply SP 800-53 controls. This is a valuable document for the manufacturing community – but its use is voluntary. In contrast, defense contractors *must* apply SP 800-171 to protect the confidentiality of CDI when they accept a contract with the DFARS -7012 clause.

NIST has also produced NISTIR 8183 (''Cybersecurity Framework Manufacturing Profile'') to assist companies to implement the NIST Cybersecurity Framework (CSF) in a manufacturing environment. Government agencies rely upon the CSF and it has earned increasing traction in many private industry sectors. But, again, use by defense manufacturers is voluntary.

DoD has updated DoDI 5000.02, with a new Enclosure 14 that addresses cybersecurity in the defense acquisition system. It makes program managers responsible to identify and protect the cybersecurity of ''enabling systems'' that include manufacturing. While program managers are instructed to pay particular attention to system elements that are vulnerable, there is no priority given to assurance that contractors who operate the factories take sufficient measures to defend against disabling or destructive attack, or to recover effectively.

In short, today there is no general practice that *assures* DoD that its *suppliers* use manufacturing-specific security tools and practices. This is true even though it is self-evident that DoD has vital interests at stake in its key defense manufacturing assets and capabilities. There is ample reason to believe adversaries have attacked defense factories and the attacks will continue. Manufacturers have a self-interest in security of their operations, of course. But trusting to market outcomes alone will not produce consistent or sufficient protection. The cost of added security may be high and the opportunity to recover on that investment – if volunteered – may be low. This leaves DoD exposed to the individual decisions of its sources and largely uninformed about their manufacturing security.

What Should Be Done?

Defense manufacturing needs to be better protected.

1. DoD should establish methods for risk assessment of defense manufacturing assets, commit resources to assist with evaluation, and make these available to trustworthy companies, at all levels, that wish to participate in the defense industrial base.

  FCR ISSN 0014-9063

a. Risk assessment should be used to identify manufacturing systems and resources with the greatest importance to production and sustainment of key defense mission and command systems.

b. Independent experts should be qualified to conduct risk assessment of key defense manufacturers and to aid in plans of action to reduce risk and enable resilience.

c. Requiring activities should be informed of the relative risk of potential manufacturers to aid in selection and award decisions and to fund stronger defenses where appropriate.

d. DoD can share the results of its risk assessment to prime and higher tier contractors, where necessary, and extend to suppliers opportunities to improve their security

2. DoD should set funds aside to assist its key contractors to implement further and better measures for manufacturing security. The DoD Manufacturing Innovation Institutes can generate new methods and new technologies to enhance manufacturing security. There are promising technologies to validate and promote. Especially for smaller companies, it may not be economic to invest in strong on-premise manufacturing security measures. Instead, DoD should facilitate use by manufacturers of secure cloud environments to support manufacturing operations. New cloud delivery techniques reduce the exposure of factory code to interception or corruption and include real-time monitoring to detect and limit attempted exploits.

3. DoD should improve its ability to collect, process and disseminate intelligence on cyber threats to manufacturing. Existing hardware and software assurance mechanisms should be leveraged to inform industry of threat vectors, defenses and recommended response. For cleared contractors, DoD can share threat-derived information as necessary, using its existing DIB Cyber Information Sharing program. DoD also can coordinate with DHS, and its existing US-CERT unit, to inform and promote industry public-private data exchange through Information Sharing & Analysis Organizations (ISAOs) specific to defense and critical manufacturing.

Even with these actions, all parts of the defense manufacturing ecosystem must be realistic. Attempts to improve perimeter defenses cannot be trusted to succeed. Measures must be taken to plan and monitor for already-embedded or future advanced persistent threats (APTs), and exercises should be regularly conducted to improve response and enable recovery when such attacks occur. In this regard, DoD should incorporate key principles from the NIST CSF, which establishes five, equally important ''Framework Functions.'' These are: **Identify**, **Protect**, **Detect**, **Respond** and **Recover**.

In today's world, where cyberattacks are diverse, serious and potentially catastrophic, manufacturers must give more emphasis to ''Respond'' and ''Recover'' so that attacks are isolated, damage contained and manufacturing output rapidly restored. In future conflicts, ''prime targets'' may be continued production by key defense manufacturers at *any* level of the supply chain. As more factories become connected to sensor-enabled networks and depend upon functionalities of the Internet of Things (IoT), the hazard grows. Owners, operators and customers need to harden manufacturing systems and enable factories to ''work through'' attacks.