ROGERS | JOSEPH | O'DONNELL

Federal Times series on supply chain security

August 13, 2018 – September 7, 2018

By Robert Metzger

	Robert Metzger is a shareholder of the law firm of Rogers, Joseph O'Donnell, PC and head of the firm's office in Washington, D.C. As a Special Government Employee of the Department of Defense, he was a member of the Defense Science Board (DSB) Task Force that produced the Cyber Supply Chain Report in 2017. He is active in other public-private initiatives, including cyber and supply chain security work for the MITRE Corporation. rmetzger@rjo.com

I. Federal supply-chain threats quietly growing

There's a lot of emphasis on cyber threats, but the government is increasingly vulnerable to gaps in supply-chain security.

August 13

II. When FISMA isn't enough

Federal agencies, especially civilian organizations, aren't going far enough to secure against cyber-physical threats to the supply chain.

August 15

III. 'Voluntary' doesn't secure the supply chain

Government contracting poses inherent supply chain threats. One agency can make a difference, but it's not who you think.

August 24

IV. Why supply-chain threats call for urgent, cooperative action

Supply-chain threats don't target only government or only industry. Confronting those threats requires a partnership — and soon.

August 31

V. Why supply chain threats require a whole-of-government response

As supply chain threats evolve across sectors, a cohesive and collaborative defense is needed.

September 7

I. Federal supply-chain threats quietly growing

By: Federal Times | 2018 08 13T19:51:24.209Z

This is the first piece in a multi part commentary series.

Nation state adversaries have exploited supply chain vulnerabilities for various hostile purposes, including theft of IP and technical data, attacks upon control systems used for electrical utilities, and manipulation of software to achieve unauthorized access to connected systems. Not enough is done to protect against the range of supply chain threats. This presents grave exposure to federal interests.

A 2013 Defense Science Board report, "Resilient Military Systems and the Advanced Cyber Threat," observed that the "challenge to supply chain management in a cyber contested environment is significant." Since that report, the challenge has only grown, and with increased dependency on "smart" devices, vulnerabilities and potential consequences have magnified. In February 2017, the DSB released a Cyber Supply Chain Task Force report, which focused on security of weapons systems against forms of supply chain attacks. This DSB report found that attack surfaces are found in the global commercial supply chain, the DoD acquisition supply chain, and the sustainment supply chain, and concluded that present capabilities to mitigate supply chain risk are limited.

Today's picture is changed because what were forecast as possibilities now are reality. Adversaries seek ways to avoid areas of U.S. dominance and to challenge U.S. interests in cyber enabled domains upon which our government, industry and populace rely. In contested cyberspace, traditional boundaries are blurred. Threats to the whole of government affect the whole of American society.

The Changing Nature of Supply Chain Threats

Just a few years ago, Congress enacted Section 818 of the 2012 National Defense Authorization Act to protect DoD against counterfeit electronic parts. The principal concern was the purchase and use of electronic parts that were non authentic and would fail when installed or used in the intended environment. Supply chain threats are now understood as broader than the example of counterfeit electronics. As shown by the well publicized experience with Kaspersky Labs anti virus software, the “software supply chain” is at risk, raising the possibility of millions of infected computers and networks.

Software increasingly defines the boundaries, operation, and security of systems relied upon by all facets of civil society – consumer facing, industrial, transportation, energy, healthcare, communications – as well as defense missions and management. The functionality of electronic systems increasingly is achieved through software. A modern airliner may have more than 10 million lines of code. A premium automobile may have 100 million lines of code operating 50 or more computerized engine control units. Electronic systems are increasingly command driven through connections to remote sensors and cloud based applications.

The co dependency of so many varieties of software dependent systems is accompanied by enlarged exposure to harm should adversaries choose to make supply chain or cyber physical attacks. As software has become more complex, many developers rely upon open sources for part of the code. In some cases, these sources are not trustworthy or no established means exist to establish trust. Should open source code be the target of malicious software insertion, great damage can be done to connected systems – and to the people and enterprises who depend upon them.

The federal government, pursuant to the Federal Information Systems Modernization Act (FISMA), has focused upon cyber threats to information and information systems. Supply chain risks extend further, to include attacks where non conforming or counterfeit parts infiltrate the supply chain, as well as cyber physical threats, by which adversaries introduce malware or exploit latent vulnerabilities in firmware or software to produce physical effects on connected or controlled systems.

These supply chain threats reach beyond public sector boundaries to include core industrial capabilities and every infrastructure component. Such threats are real and present – as evidenced by recent headlines.

The New York Times reported on March 15, 2018, that the Trump Administration accused Russia of cyberattacks 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'" on 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."

Robert Metzger is a shareholder of the law firm of Rogers, Joseph O'Donnell, PC and head of the firm's office in Washington, D.C. As a special government employee of the Department of Defense, he was a member of the Defense Science Board (DSB) Task Force that produced the Cyber Supply Chain Report in 2017. He is active in other public private initiatives, including cyber and supply chain security work for the MITRE Corporation.

II. When FISMA isn't enough

By: Federal Times | 2018 08 16T01:31:46.580Z

This is part two in a multipart commentary on supply chain security. For part one, click here.

Federal departments and agencies are obligated by the Federal Information Security Modernization Act to protect the confidentiality, integrity and availability of defined categories of federal information ("controlled unclassified information," or CUI) and information systems that host, process or transmit that information. But it's often not enough to secure the federal supply chain against software threats and cyber physical dangers.

FISMA is directed to protect against network and information system attacks that can compromise federal CUI. Present federal efforts give comparatively little attention to cyber physical threats, such as corruption of firmware or other types of software that produce unwanted and adverse effects on connected equipment. Measures intended to protect IT, even where successful, may do little to secure operational technology.

Spurred by Congress, DoD requires its larger contractors to implement systems and procedures to detect and avoid counterfeit electronic parts. On its own initiative, DoD has implemented DFARS procurement regulations and contract requirements to make all DoD suppliers safeguard controlled technical information of military or space significance and other CUI types, using NIST security principles.

DoD's acts concern the risk that the supply chain might deliver counterfeit parts and the cyber threat to the confidentiality of information and information systems that host CTI and other forms of CUI. To protect contractor information systems against network delivered attacks, DoD requires contractors to employ the 110 safeguards of NIST Special Publication 800 171.

The present challenge is to identify, detect, defend against, respond to or recover from software delivered cyber physical attacks on operational technology – for example, industrial control systems, supervisory control and data acquisition, programmable logic controllers and other systems that operate manufacturing facilities and infrastructure. SP 800 171 is not intended to protect these systems.

Civilian departments have done less than DoD against supply chain threats. For years, civilian agencies have considered a counterpart to the DoD “cyber DFARS” to require protection of CUI when shared with non federal entities. There currently is no such regulation or requirement, but an inter agency effort is proceeding that may produce a regulation, like the “cyber DFARS,” requiring use of NIST SP 800 171 safeguards by non federal entities to protect all CUI they receive it from a federal agency.

DoD presently has special authorities, to avoid counterfeit electronics and exclude high risk sources, not available to all federal departments and agencies. Generally, civilian agencies take no regular and direct measures, beyond ordinary quality and conformance requirements, to require suppliers or service providers to secure their supply chains or to report and remedy supply chain attacks. But adversaries will not limit hostile activities to the defense sector.

The president’s executive order from May 11, 2017, holds heads of executive departments accountable for managing cybersecurity risk to their enterprises and calls on the executive branch to support the cybersecurity efforts of the owners and operators of critical infrastructure. It further requires a report on the cybersecurity risks facing the defense industrial base, including its supply chain. These are commendable in intent, but more policies, efforts and reports do not produce objective improvements in security, nor do they necessarily change the security practices of commercial enterprises.

It’s critical to recognize threats to private industry affect government interests. Federal action on cyber and supply chain threats focus upon federal information systems and contractors for supplies, systems or services. Attacks upon utilities or transportation facilities, or other aspects of critical infrastructure can produce discomfort, inconvenience, economic loss, property damage or even personal injury or death. Attacks upon civil logistics providers, even where facilities are located in the continental United States, can inflict damage on defense business and erode the ability of commanders to deploy forces and execute missions on foreign soil.

Robert Metzger is a shareholder of the law firm of Rogers, Joseph O'Donnell, PC and head of the firm's office in Washington, D.C. As a special government employee of the Department of Defense, he was a member of the Defense Science Board (DSB) Task Force that produced the Cyber Supply Chain Report in 2017. He is active in other public private initiatives, including cyber and supply chain security work for the MITRE Corporation.

III. ‘Voluntary’ doesn’t secure the supply chain

By: Federal Times | 2018 08 24T19:37:56.248Z

This is part three in a multipart series on supply chain security. Click here for part one and part two.

The federal government encourages many forms of voluntary security measures. The National Institute of Standards and Technology has produced a voluntary cybersecurity framework that is a useful way to organize, achieve and measure security progress. But voluntary measures are insufficient when not everyone is adopting the measures.

Adversaries can and will exploit resulting gaps and wreak widespread injury through supply chain attacks directed against weak links, such as market participants indifferent to security. This exposure, unfortunately, also is present in the Department of Defense’s efforts to improve the cybersecurity of defense industrial base contractors. There, NIST Special Publication 800 171 safeguards are specified — but there is no method of assurance or assessment beyond “trust” in contractors to comply with contract terms.

An unfortunate truth about supply chain vulnerability — and especially software supply chain exposure — is the enormous attack surface and the virtually limitless number of points where an attack can be executed. Adversaries can avoid the best defended resources and most secure products (or components) and instead find weak actors and exploit insecure entry points.

Procurement measures are significant. but not sufficient

DoD has been the leader in efforts to defend against supply chain exposure. Even so, experience shows that procurement methods may not achieve effective supply chain security across the entire range of exposure.

By definition, procurement measures, such as federal acquisition regulations or contract clauses, affect only those in the chain of contract with the federal agency customer. While the universe of companies affected by DoD procurement measures is significant, it nonetheless represents a very small fraction of U.S. enterprises at risk.

Even where procurement methods matter, such as in DoD procurements and those of other federal agencies, today's emphasis is on price, schedule and performance. Security requirements may be tacked on to new solicitations for supplies and services, but federal purchasers, at present, evaluate the cyber and supply chain security of contractors only in limited instances.

Federal leaders should elevate security to the point that it becomes the "fourth pillar" of the acquisition process – equal in priority to cost, schedule and performance.

Software supply chain attacks: discrete targets, broad effects.

Conventional thinking has been that adversaries seek high "return on investment" by targeting supply chain attacks in ways that achieve precise, impactful effects. The publicly reported experience with Kaspersky Labs software, however, suggests an alternative paradigm that is very dangerous: infiltration through widely installed, publicly accessible software.

Measures confined to government contractors, or which are voluntary for commercial enterprises, do little to mitigate and certainly do not defeat such threats. Commercial sources of supplies or services for government use can be unwittingly exposed to tainted, commercial origin, widely marketed software and, conceivably, firmware in widely utilized devices.

No part of the "system development life cycle" is unexposed to software delivered supply chain attack. Contemporary systems typically depend upon a global supply chain for parts and for software, including open source components from sources both known and unknown. There is exposure at all points along the life cycle spectrum, from inception to end of life disposition.

Even industrial base issues come into play here, as the U.S. becomes increasingly dependent upon foreign sources for critical, high performance microelectronics.

IoT: Internet of Threats

The Internet of Things is producing massive interconnection of sensors, devices and systems – and massive interdependencies among systems. Literally billions of connected devices are in our near term future. With this connectivity, paths for attack, malware propagation and distribution grow exponentially. Detection and response to such attacks implicates many federal agencies, notably the FCC.

The FCC has a pivotal role in security of our increasingly interconnected national economy. It is the "gatekeeper" for the communications instrumentalities upon which connected systems rely in private sector and for much of the public sector.

Apart from authority to hold regulated communications service providers to higher security standards, the FCC can play an important role in shaping future network architecture so that transport layer attacks are rapidly identified and isolated — helping to mitigate the risk of "cascading" impacts across connected systems. The FCC will also have a key role in protecting U.S. interests in the development of the 5G mobile networks standard, where other nation states may seek outcomes adverse to the U.S.

Robert Metzger is a shareholder of the law firm of Rogers, Joseph O'Donnell, PC and head of the firm's office in Washington, D.C. As a special government employee of the Department of Defense, he was a member of the Defense Science Board (DSB) Task Force that produced the Cyber Supply Chain Report in 2017. He is active in other public private initiatives, including cyber and supply chain security work for the MITRE Corporation.

IV. Why supply chain threats call for urgent, cooperative action

By: Federal Times | 2018 08 31T16:46:09.730Z

This is part four in a multipart series on supply chain security. Click here for part one, part two and part three.

The potential consequences of supply chain attack are severe. Recent attention has focused on hacks resulting in exposure of private information — Sony in 2014, the Office of Personnel Management in 2015 or Equifax in 2017. The loss of confidentiality of millions of personal records, and the resultant impacts upon individual privacy, are matters of great national concern.

A successful cyber physical attack upon national infrastructure could have even worse consequences. Such attacks already have been attempted (and publicly reported) by Russia as well as Iran. Should such attacks succeed, they will produce widespread physical effects — destruction of equipment or facilities, and crippling or loss of key public assets — affecting the functioning of government, the strength of our economy, and the daily lives of millions of U.S. citizens.

The national interest is to defend against and recover from supply chain attacks. A supply chain directed attack need not be confined to one server, one information system, one agency or enterprise, or one type of private record. Adversaries may mount simultaneous or sequential attacks on diverse industry and government sectors, related or not, with objectives that may include confusion, public frustration and leadership doubt.

Defense against such attacks and remediation requires stronger action than contract requirements and voluntary measures. Sectoral initiatives can be helpful, but they may not scale to cover the threat's complexity or severity. Nor do they address cross or multi sectoral impacts.

The time to improve defenses, plan for attack, and prepare to recover is now. Waiting to act until after the event(s) is a recipe that adversaries can exploit now to their advantage. The situation today is what was predicted — and feared — just a few years ago. Restraint on the part of adversaries is unlikely, and certainly cannot be assumed. Deterrence has a role, but its operation is complicated by the "gray" nature of asymmetric conflict in cyber domains and the continuing difficulty of attribution to attackers.

Resolving tensions between government and industry

Congress has been reluctant to impose security upon the commercial sector by law or regulation. Industry has concerns about the costs and burdens of federal intervention and prefers to be free to use its superior abilities, agility and technology to deal on its own with supply chain and cyber threats.

Government and industry must work together to defend against and defeat these threats. But the stakes are too high, and the risks too great, for government to defer to industry and hope that market forces alone will produce sufficient results.

At the very least, Congress should require measures now that anticipate attack and enable prompt, effective response in the event of emergency. Threats are not directed at the government distinctly from industry. Government and industry share interests in finding common grounds and shared methods for cooperative, mutual defense.

- There is no reason other than optimism uninformed by experience to trust that only voluntary measures in the private sector will provide the needed protection to critical infrastructure. Even if some companies do it "right," or even "better" or "best," adversaries will attack the weaker links – and there are many enterprises indifferent to security.
- Leaders in industry will assert that they can do it better, smarter, with more agility, and with better results. That may well be true — but only for the leaders. Even then, the security of the enterprise at the end point of the supply

chain does not mean that assurance extends to connected systems or to all participants in regulated industry. Incentives are needed to promote best practices in supply chain security in the private sector.

- As industry and government share exposure and will suffer similar or the same consequences of supply chain attacks, it is critical to promote means for partnership so that the private and public sectors cooperate in mutual defense and remediation when attacks occur.

Robert Metzger is a shareholder of the law firm of Rogers, Joseph O'Donnell, PC and head of the firm's office in Washington, D.C. As a special government employee of the Department of Defense, he was a member of the Defense Science Board (DSB) Task Force that produced the Cyber Supply Chain Report in 2017. He is active in other public private initiatives, including cyber and supply chain security work for the MITRE Corporation.

V. Why supply chain threats require a whole-of-government response

By: Federal Times | 2018 09 07T20:17:10.010Z

This is the final part in a multipart series on supply chain security. Click here for part one, part two, part three and part four.

Supply chain security is a problem that crosses traditional boundaries. One sector can be exposed to or impacted by an attack upon another, or even be used as a vehicle. Lines between cyber effects and physical results are blurred by the nature of cyber physical attacks that use software to deny, damage or destroy physical assets.

Hostile nations can conduct asymmetric warfare by use of supply chain directed attacks as surrogates or alternates for conventional military power. In this context, defense of the homeland requires actions coordinated among the civilian agencies, the Department of Defense and the intelligence community.

Cross agency action on threat information is needed. Adversaries' tactics, techniques and procedures in supply chain attacks are known or knowable to the IC and other specialized assets of the U.S. government. Methods to deter or respond to such attacks may reside in the DoD and its components. The National Protection and Programs Directorate (NPPD) of DHS has many responsibilities and resources for protection of domestic infrastructure and industry.

Understanding how an adversary may attack, its methods, and where attacks have been attempted (globally) is key to informing deflection of threats, detection of events, protection and recovery. An effective national response to supply chain threats utilizes all source intelligence and coordinated collection and analysis. Both DHS and DoD now are moving in this direction.

Reforming, empowering, evaluating

There is widespread enthusiasm for measures that will “reform” federal procurement to reduce barriers to commercial sources, encourage innovation, speed purchase and delivery, and eliminate the regulatory cost premium.

In the 2016 National Defense Authorization Act, Congress authorized an independent advisory panel on streamlining and codifying acquisition regulations (the “section 809 panel”). Improved security was not in the charter of the section 809 panel, but there is potential tension between security objectives. That can add time, expense and federal specific demands to acquisitions, and the objectives of section 809 and similar reform efforts.

The solution may be to establish risk informed categories for DoD procurement such that greater security obligations are imposed upon the “higher” tiers but minimized for commodity, commercial off the shelf and other low risk items.

Congress allows DoD to exclude “high risk” supply chain sources, and now DoD is working to better utilize that authority. The Kaspersky Labs example is one where national interest led to the exclusion of a suspect source.

Reportedly, DoD is now working on a software “do not buy” list. Congress is looking at extending this authority to other departments and agencies, and at other measures to prevent contracting with the enemy on a whole of government basis.

Such initiatives will have significant effect upon thousands of private sector enterprises. Agencies need to improve coordination to produce consistent goals, uniform measures and fair process. NIST can play an especially important role here, given the widespread private sector use of the cybersecurity framework.

Agencies should wield the power

As the threat environment worsens, regulatory agencies should be ready to use their authority on a coordinated basis to improve supply chain defenses, promote resiliency and enable recovery. While regulatory agencies have limited purchasing leverage, they have sweeping authority over enterprises subject to their oversight.

In some cases, regulatory agencies can condition market access upon or otherwise mandate security measures. They have authority over market entry, licensing, approvals, qualification, eligibility and more. They should use that authority to inform, instruct, enable, and assess self improvement. But they should hold in reserve the authority to require improved security.

International measures require multi agency coordination. There are distinct U.S. interests in protecting supply chain security for our Government, and for our national economy. But supply chain security also affects our allies and other trading partners; truly, it is an international problem.

Ultimately, the U.S. cannot “go it alone” or separate itself from a global supply chain.

For this among many other reasons, solutions to supply chain risks will involve international cooperation. Important measures may be achieved through international agreement, and international organizations will play a critical role in setting standards and best practices. It may be advantageous to U.S. interests to promote a council of allied countries to exchange information about supply chain vulnerabilities and responses.

Past doctrines, historical methods and legacy techniques have limited value today. Conventional thinking needs to change to confront the contemporary threat environment. New actions are necessary to challenge orthodoxy and adroitly secure the supply chain.