Proposals for FY19 NDAA Section 889(a)(1)(B) Regulation
June 2, 2020

This paper makes proposals for the regulation implementing FY19 NDAA Section 889(a)(1)(B).[1]

- Section I of this paper describes the significant scoping problem raised by the law, including hypothetical but likely examples, and proposes definitions to address it.

- Section II addresses the designation of additional covered companies – both subsidiaries of Huawei/ZTE and otherwise – and proposes a significant role for the Federal Acquisition Security Council ("FASC").

- Section III explains why Section 889's waiver authority does not help to address the scoping problem.

- Section IV briefly addresses legal and procedural issues.

Procedurally, Congress and the Administration should delay the effective date of Section (a)(1)(B) by one year until August 13, 2021. Meanwhile, the implementing regulation should be issued in draft form – not an "interim final rule" – to give stakeholders ample time to comment. The complexity of the issues involved, the need for companies to have time to implement the rule internally, and the current statutory deadline all suggest that the draft rule be published for comment as soon as possible.

I. The Scoping Problem: Examples and Solutions

Examples. Section 889(a)(1)(B) prohibits federal agencies from contracting with any **entity** that **uses** any **equipment, system, or service** that **uses** covered telecommunications equipment or services – mainly Huawei and ZTE ("H/Z") plus certain video surveillance equipment ("VSE") manufacturers[2] – as a substantial or essential component. This will have the following consequences, as shown via these hypothetical but likely examples:

- Company A is an information technology company with a sales office in the United Kingdom. The company uses a shipping vendor, such as the Royal Mail, to ship its

[1] John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 889, Pub. L. No. 115-232, 132 Stat. 1636, 1917 (Aug. 13, 2018).

[2] Covered VSE includes, "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company…." Sec. 889(f)(3)(B).

products. The Royal Mail uses (hypothetically) H/Z equipment in its enterprise networks. *Company A is barred from selling to the U.S. government.*[3]

- Company B is a manufacturer of personal protective equipment (PPE) with operations in the U.S. and southeast Asia. The overseas division obtains network service for its Asian plant from a local provider that uses H/Z gear. *Company B is barred from selling to the U.S. government.*

- Company C is a pharmaceutical company with a drug manufacturing plant in India. The company provides its Indian employees with cell phone service through an Indian ISP such as Bharti Airtel. Bharti Airtel uses H/Z equipment. *Company C is barred from selling to the U.S. government.*

- Company D is a small, woman-owned, IT reseller that sells H/Z equipment or covered VSE to her non-federal customers.[4] *Company D is barred from selling to the U.S. government* because "use" may include the act of selling.

- Company E is an auto parts company based in rural America that receives data or cell service from a small provider that has H/Z equipment in its networks. Based on public declarations made to the FCC in 2018, this includes parts of at least the following states: AL, CO, ID, KS, KY, MT, NE, ND, SD, TN, UT, and WY.[5] *Company E is barred from selling to the U.S. government.*

    - Congress and the FCC are attempting to remove H/Z gear from U.S. networks through the Secure and Trusted Communications Networks Act. However, the law gives carriers one year after the receipt of grant funds to remove the H/Z gear,[6] and Congress has not yet appropriated the necessary funding.

[3] While a shipping service likely "cannot route or redirect user data traffic," Company A's use of a non-telecommunications service such as shipping is not permitted by the exclusion in Section 889(a)(2)(B). First, the exclusion is limited to "telecommunications equipment" only. Second, the phrase "Nothing …. shall be construed to … *cover* telecommunications equipment" implies that the exception was intended to modify only the phrase "*covered* telecommunications equipment and services" rather than the phrase "any equipment, system, or service."

[4] This could include, for example, a small security installer and reseller that provides camera systems to local convenience stores along with federal customers like the local Social Security office.

[5] Comments of Competitive Carriers Association, filed June 1, 2018 in WC Docket No. 18-89, at Appendix (declarations of small providers). The following carriers made declarations stating, among other things, that they provide service in portions of the states indicated: SI Wireless d/b/a MobileNation (KY, TN), Viaero Wireless (CO, KS, NE, SD, WY), James Valley Telecommunications (SD), United Telephone Association (KS), Nemont Telephone Cooperative d/b/a Sagebrush Cellular (MT, ND, WY), Pine Belt Cellular (AL), Union Wireless (CO, ID, UT, WY).

[6] Secure and Trusted Communications Networks Act § 4(d)(6)(A), Pub. L. No. 116-124 (Mar. 12, 2020).

- Company F is an American business (any size, any place) that relies on a non-carrier service that uses H/Z enterprise gear in its data centers, enterprise networks, etc. *Company F is barred from selling to the U.S. government.*

    - The extent of non-carrier enterprise use of H/Z products in the United States is unclear, and the Secure Networks Act did not attempt to replace such use even in the United States.

- Company G is a chemical manufacturer with both federal and non-federal customers. It uses covered video surveillance equipment to monitor its facilities either in the U.S. or overseas, **or** has a supplier that uses covered VSE.[7] *Company G is barred from selling to the U.S. government.*

    - Video surveillance equipment from the prohibited manufacturers currently accounts for 25-40% of all commercial VSE installed in the United States.

Substantial or essential. Notably, the phrase beginning with "substantial or essential" at the end of Section 889(a)(1)(B) does not alleviate the scoping problems identified above. This is because the "substantial or essential" phrase modifies the second occurrence of the word "use" in the provision, not the first.[8] For example, Company A would be barred due to the Royal Mail's

[7] Video surveillance for a chemical plant constitutes the "physical security of critical infrastructure," thus making Section 889(f)(3)(B) applicable. *See* CISA, *Critical Infrastructure Sectors*, https://www.cisa.gov/critical-infrastructure-sectors (listing the chemical sector as a critical infrastructure sector).

If the manufacturing occurs overseas, it is unclear whether security for those plants constitutes the "physical security of critical infrastructure" under the statute. For example, Presidential Policy Directive 21 (PPD-21) required the State Department to "engage foreign governments … to strengthen the security of *critical infrastructure located outside the United States*" and refers to "the resilience of critical infrastructure on which the Nation depends." Barack Obama, *Directive on Critical Infrastructure Security and Resilience, Presidential Policy Directive/PPD-21*, Feb. 12, 2013, 2013 Pub. Papers 106, 109 (emphasis added); *see also id.* at 110 (similar directive to FCC). However, the statutory definition of "critical infrastructure," cited in PPD-21, is "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." USA Patriot Act of 2001 § 1016(e) [42 USC 5195c(e)]. Ideally, the regulation should clarify this.

[8] Two canons of statutory construction support this reading. First, the "last-antecedent rule" states that the descriptive phrase modifies the last adjacent term to which it could apply – here, the second "use." Second, an identical phrase in subparagraph (A) clearly applies the "substantial or essential" phrase to modify what appears as the second "use" in subparagraph (B), and the statute must be read consistently as a whole. *See generally* Antonin Scalia & Bryan Garner, *Reading Law* (2012); *see also* here (online resource excerpting Scalia & Garner).

substantial use of H/Z, even as it does not matter whether Company A's use of the Royal Mail is substantial or not.[9]

Outcomes. The examples illustrate that compliance with Section 889(a)(1)(B) is not possible without appropriate scoping constructions. Virtually every federal contractor would either be unable to certify compliance, or in doing so would subject itself to liability under the False Claims Act.[10] For larger companies, an already-impossible task is further complicated by operations in multiple countries and across various business units. For federal contractors of all sizes, lack of awareness regarding the statutory scoping problem will create liability.

Definitions. To address the problems above, the rule implementing Section 889(a)(1)(B) should include the following definitions:

- ***Use*** means use that is (i) knowing; (ii) by an entity; (iii) in the United States; and (iv) in fulfillment of the contract.

- ***Entity.***
    - Option A: *Entity* means the legal entity that executes the contract and does not include parents, subsidiaries, or affiliates of that entity.
        - Variant: *Entity* does not include any parent, subsidiary, or affiliate of such entity.

    - Option B: *Define "entity" based on Commercial and Government Entity (CAGE) code, which would typically exclude parents / subsidiaries / affiliates.*[11]
        - Variant: *Use SAM Managed Identifiers (SAMMI),*[12] *DUNS numbers, or other ID numbers that clearly distinguish between parents / subsidiaries / affiliates.*

- ***System*** means a system used in fulfillment of the contract.

[9] The "substantial and essential" phrase likely protects "use" of H/Z products for testing and research purposes, but the regulation should clarify this. U.S. companies often use H/Z equipment for research and testing purposes, or even to evaluate the security of H/Z products.

[10] *See, e.g.*, GSA, *Summary of Findings and Feedback*, Nov. 6, 2019, at 6, 9-10 (discussing False Claims Act and general risks to businesses).

[11] *Cf.* DOD, GSA, and NASA, *Federal Acquisition Regulation; Commercial and Government Entity Code*, 79 Fed. Reg. 31,187 (May 30, 2014). When the FAR Council established the CAGE code requirement, it explained that "[t]he final rule requires a CAGE code assignment for the entity (with its specific name and physical address) to whom the Government awards the contractual instrument, i.e., that entity noted on the front page of the contract document." *Id.* at 31,188. The rule distinguishes the contractor's own CAGE code from its "immediate and highest-level owner's CAGE codes and legal names." *Id.*

[12] *See* GSA Blog, *Done with DUNS*, Mar. 26, 2019, https://gsa.federalschedules.com/blog/done-with-duns/

- ***Fulfillment of the contract.***
    - Option A: Equipment, systems, or services are used 'in fulfillment of the contract' if the contract requires: (i) their use, or (ii) to a significant extent, their use in the performance of a service or the furnishing of a product. *See* FAR 2.101, Definitions, *Information Technology*.[13]
        - Variant: Equipment, systems, or services are used 'in fulfillment of the contract' if they are used in the performance of services under the contract or the furnishing of a product under the contract.

    - Option B: Equipment, systems, or services are used 'in fulfillment of the contract' if they are used to collect, develop, receive, transmit, or store agency data in support of the performance of the contract. *See* DFARS 204.7301, Definitions, *Covered defense information*.[14]

    - Option C: *Other concepts that capture the concept of nexus to federal data while being cognizant of how networks operate*.[15]

    - Note: *To further remove doubt – and regardless of which option is chosen – add a sentence explicitly excluding non-performance use that incorporates a non-exhaustive list of examples such as billing.*

- ***Substantial or essential component*** means any component used in the fulfillment of the contract that is necessary for the proper function or performance of a piece of equipment, system, or service.
    - Variant: *Substantial or essential component* means any component of a system used in the fulfillment of the contract that is necessary for the proper function or performance of a piece of equipment, system, or service required for the fulfillment of the contract.

[13] https://www.acquisition.gov/content/2101-definitions

[14] https://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

[15] As with every option, any construction based on data flow requires careful analysis. For example, if a contractor provides services to a U.S. civilian agency overseas, such services might include secure transmission of data back to the United States via encrypted tunnels (VPNs). Even if the contractor controls both ends of the tunnel, the encrypted packets would potentially be transmitted via routers in other countries. Such "use" of open networks would run afoul of Section 889(a)(1)(B), although the interconnection exclusion in paragraph (2)(A) would potentially apply *if* the exclusion is construed sufficiently broadly by the regulation. If the interconnection exclusion does not apply, then "use" would need to be "knowing use."

Analysis. The definitions above are intended to help serve the statute's objective of enhancing the security of federal agency data flow while avoiding scoping problems.[16] However, not every word or clause above may be necessary to resolve the scoping problem, particularly if the government believes any clause would raise a specific federal data security concern. For example:

- "in the United States" could potentially be dropped if other concepts in the definitions of "entity" and "use" are incorporated;
- "knowing" would be very practically helpful but may not be necessary if other concepts are included in sufficient degree; and
- the "system" and "substantial or essential component" definitions may not be needed depending on what other choices are made.

Ultimately, the final choice of definitions must be based upon careful consideration of specific hypotheticals in order to achieve the statutory objective while avoiding scoping problems.

II. Using the FASC to Help Further Congressional Intent

Role of the FASC. Until recently, federal supply chain security concerns about specific companies were handled in an ad-hoc manner without a framework, including legislation specifically targeting Kaspersky Lab as well as Section 889 which primarily targets Huawei and ZTE. In December 2018, Congress enacted the Federal Acquisition Supply Chain Security Act ("Supply Chain Security Act")[17] to provide a structure for a coordinated, government-wide process. The Act created the Federal Acquisition Security Council (FASC) which incorporates expertise from various agencies collectively well-positioned to assess acquisition-related security and counterintelligence risks. Moreover, the FASC is well-positioned to balance such risks against the potential costs and operational consequences of a particular procurement restriction, and the Supply Chain Security Act also incorporates due process protections.

The Supply Chain Security Act charged the FASC with developing criteria and processes for supply chain information sharing to improve federal agency supply chain risk management efforts. In addition to its policymaking function, the FASC can recommend the government-wide exclusion or removal of concerning products and services to the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence. It is comprised of senior officials from OMB, GSA, DoD, DHS, and the intelligence community that have expertise in supply chain risk management, acquisitions, or information and communications technology.

[16] The underlying purpose of enhancing the security of federal data flow can be readily discerned, and especially from the exceptions. For example, Section 889(a)(2)(B) would even allow the use of some H/Z equipment in federal systems provided that the equipment cannot route, redirect, or permit visibility into data.

[17] Pub. L. No. 115-390, title II (Dec. 21, 2018).

FASC and Section 889. Section 889 – which was enacted *before* the Supply Chain Security Act – provides authority to the head of each federal agency to implement it. However, most agencies would not be in a position to exercise this authority appropriately on their own. Since Congress has since established the FASC and charged it with handling such tasks comprehensively, the regulation should therefore adopt a systemic role for the FASC to guide implementation of Section 889. Specifically, agency authority under Section 889 should be exercised only pursuant to a recommendation from the FASC.[18]

Additional Chinese companies. Section 889(f)(3)(D) allows the Secretary of Defense to designate additional Chinese companies beyond those explicitly named as "covered." The FASC process is intended to identify such companies, and also offers a due-process mechanism to protect any company that may be inappropriately designated. The implementing regulation should therefore require that any further designation of covered companies by DOD under Section 889(f)(3)(D) will be made pursuant to the process by which the FASC recommends, and agencies issue, exclusion or removal orders.

Time to implement. The addition of new covered companies – whether newly-discovered Huawei or ZTE subsidiaries or other entities – will pose implementation issues for contractors if and when the government adds to the list. If the government designates additional covered companies under Section 889(f)(3)(D), the regulations should ensure that federal contractors have a sufficient amount of time before compliance is required. The government should also undertake appropriate efforts to inform all federal contractors of any additional designations.

Huawei & ZTE subsidiaries. Section 889(a)(1)(B) includes not just Huawei, ZTE, Dahua, Hytera, and Hikvision, in the definition of "covered" equipment, but also subsidiaries and affiliates of those companies. The U.S. government has the ability and is best-positioned to identify those subsidiaries and affiliates – and has already done so in one case.[19] To address this, the regulation should include the following definitions:

- ***Subsidiary or affiliate*** means, for purposes of the definition of the term "covered telecommunications equipment or services" only, any subsidiary or affiliate identified by an executive agency as a segment.
    - Variant: substitute "the Federal Acquisition Security Council" in place of "an executive agency."
    - Variant: add the word "known" before "subsidiary or affiliate."

- ***Segment*** has the meaning defined in section 2.101 of the Federal Acquisition Regulation.

[18] Ideally, Section 889 would be amended to incorporate the Supply Chain Act process. At a minimum, the regulations should require that agency heads consult the FASC prior to making any determination under Section 889.

[19] Department of Commerce, Bureau of Industry and Security, *Addition of Entities to the Entity List*, 84 Fed. Reg. 22,961 (May 21, 2019) (identifying 60-plus global entities as affiliates of Huawei).

III. Waivers

Section 889(d) provides a very limited waiver authority to the government. Any exercise of this authority is subject to very significant statutory constraints:

- "One-time basis" for a period of "not more than two years"
- Entity seeking waiver must provide a "compelling justification"
- Entity must provide a "full and complete laydown" of the presence of covered equipment in the entity's "supply chain"
    - "Supply chain" is not defined, and could therefore include literally anything
- Authority is exercised by "the head of an executive agency" rather than government-wide
    - Administration directives could possibly supersede this, but not the other points above

Due to these significant constraints, the waiver authority in subsection (d) is inherently unsuitable to permanently addressing the scoping problems described above. In short, what is impossible today will still be impossible tomorrow.

Delayed effective date. A blanket waiver directed by the Administration, *i.e.* a "deemed-granted" approach, could potentially be used as a temporary mechanism to delay the effective implementation of Section 889(a)(1)(B) for all contractors. However, even this would likely carry significant drawbacks. For example, the "full and complete laydown" condition – which is mandatory – cannot be satisfied since contractors would need to provide information that is essentially impossible to obtain, per the hypothetical examples above. Furthermore, the "one-time" limit would mean that no entity would be eligible to seek another individualized and legitimately-needed waiver for any other reason.

Implementation. While the waiver provision is not suitable for addressing the overall scoping problem, it does provide an important safety valve for more specific situations. To provide clarity, the regulation should therefore provide definitions for all key terms in Section 889(d), including "compelling justification," "full and complete lay down," "phase out plan," and what is an "entity that requests such a waiver." For example, an evaluation of "compelling justification" should consider the following factors:

1. Whether the entity operates in a geography where covered equipment is the only option;
2. Whether the system using covered equipment is air-gapped or otherwise disconnected from the system or business unit contracting with the government entity;
3. Whether the entity presents a detailed supply chain risk management (SCRM) plan outlining how it is able to neutralize any risk involved with using covered equipment.[20]

[20] Some of these factors may be more or less relevant depending on which scoping definitions are ultimately chosen.

In addition, since waivers are exercised by "the head of an executive agency," the regulation should clarify how entities providing goods or services under a Government-Wide Acquisition Contract (GWAC) such as GSA Schedule 70 or NASA SEWP can obtain a waiver, as obtaining a waiver from every federal agency head individually is either impossible or highly impractical. Finally, the regulation should protect proprietary information that companies may include in their waiver submissions.

IV. Legal Authority, Congressional Intent, and Process

Legal authority and congressional intent. Congress wrote the statute broadly so that agencies could take appropriate steps to "find things Congress missed" if necessary to secure federal data flows. However, Congress also intended for agencies to make the statute workable, which it currently is not. While arguments could be made that the definitions proposed above may significantly alter the meaning of some words, the underlying purpose of the statute clearly necessitates *some* regulatory intervention.

At least two legal arguments support such intervention. First, a well-known canon of statutory construction calls for avoiding absurd results – here, the termination of all federal procurement in August 2020. The mere fact that such termination is a potential outcome of the statutory text clearly invests the agencies with *some* legal flexibility to adopt an interpretation that avoids this outcome. Second, the principle of *Chevron* deference allows agencies to interpret ambiguous statutes, and the lack of definitions for key terms surely suggests such ambiguity. Under *Chevron*, the FAR Council's reasonable interpretation of the statute will receive deference should judicial review of the regulation ever be invoked.

Time for comment before effective date. Last but certainly not least, industry needs sufficient time to comment on a draft rule well before it takes effect. A draft proposed rule should be issued promptly that provides a sufficient period for comment. Careful analysis of any proposed rule text will be essential, including time for considering appropriate hypotheticals such as those presented above. This was not the case in the rule implementing Section 889(a)(1)(A), which was issued as an interim rule on the very day of its effective date.[21] As described above, subparagraph (B) presents significantly more difficult issues.

Phased Implementation. Ultimately, implementation of any regulation will take more time than is available before the current statutory deadline. Congress and the Administration should therefore delay the effective date of Section 889(a)(1)(B) by one year until August 13, 2021, largely owing to support for and challenges associated with COVID-19.

[21] 84 Fed. Reg. 40,216 (Aug. 13, 2019), https://www.govinfo.gov/content/pkg/FR-2019-08-13/pdf/2019-17201.pdf