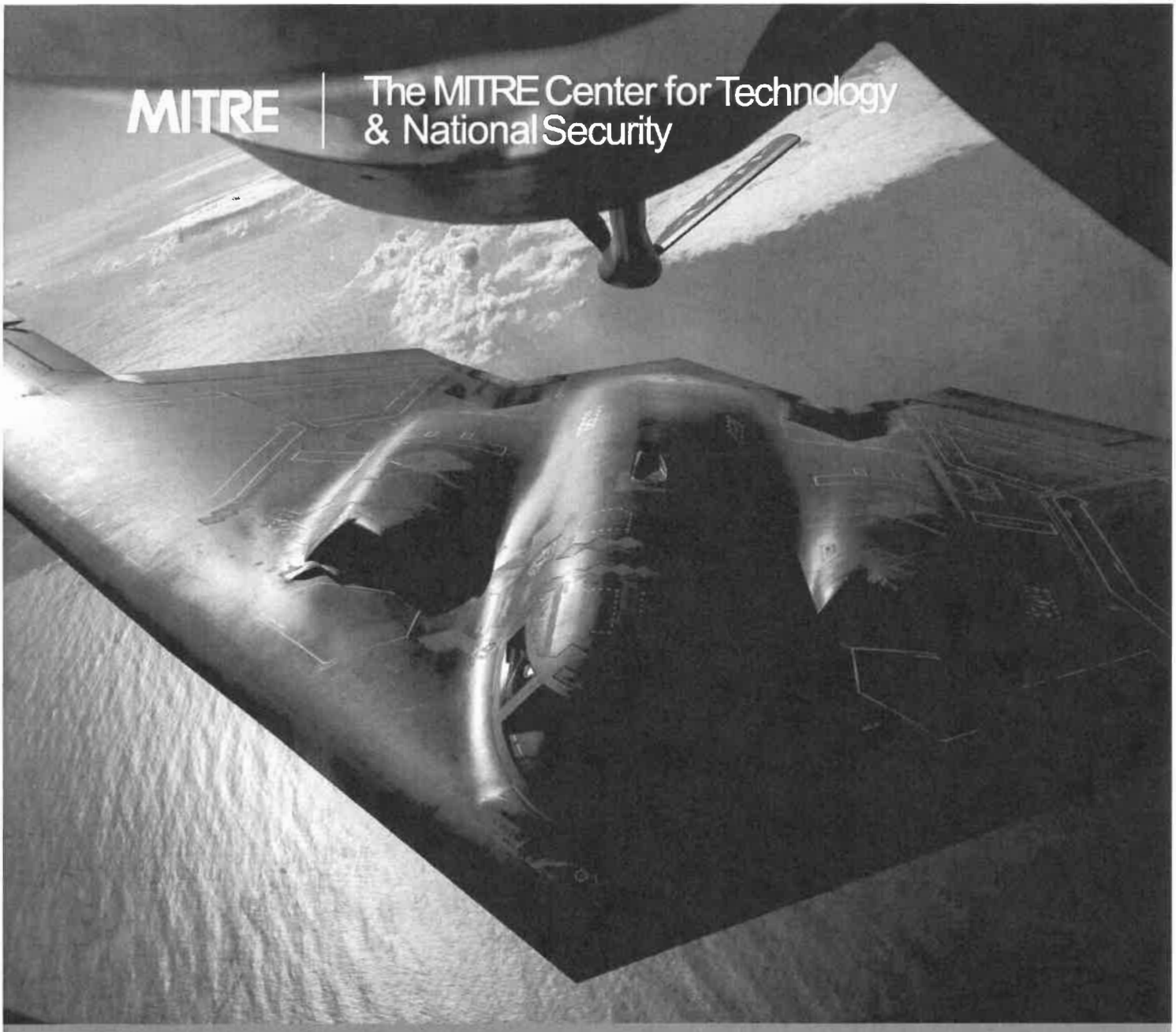
Pub K

PUBLIC CONTRACTS

Annual Review Cybersecurity and IT Supplementary Materials

Table of Contents



DELIVER UNCOMPROMISED

A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War

By Chris Nissen, John Gronager, Ph.D.,
Robert Metzger, J.D., Harvey Rishikof, J.D.

This page intentionally left blank.

Executive Summary

The character of war is changing. Our adversaries no longer have to engage the United States kinetically. They have shifted their strategy to engage our nation *asymmetrically,* exploiting the seams of our democracy, authorities, and even our morals. They can respond to a kinetic action non-kinetically and often in misattributed ways through *blended operations* that take place through the supply chain, cyber domain, and human elements.[1] They can render our national capability to project power—hard or soft—non-mission ready and collapse and even reverse the decision cycle.

Deliver Uncompromised

"For mission owners, the primary goal of DoD must be to deliver warfighting capabilities to Operating Forces without their critical information and/or technology being wittingly or unwittingly lost, stolen, denied, degraded or inappropriately given away or sold."

William Stephens, Director of Counterintelligence, DSS

Today, various parts of the Department of Defense (DoD) and the Intelligence Community (IC) are generally aware of cyber and supply chain threats, but intra- and inter-government actions and knowledge are not fully coordinated or shared. Few if any holistically consider the entire blended operations space from a counterintelligence perspective and act on it. Risk quantification and mitigation, as a mission, receive insufficient resources and prioritization. Too little attention is directed toward protection of operational security or software assurance. There is no consensus on roles, responsibilities, authorities, and accountability. Responsibilities concerning threat information are "siloed" in ways that frustrate and delay fully informed and decisive action, isolating decision makers and mission owners from timely warning and opportunity to act.

DoD must make better use of its existing resources to identify, protect, detect, respond to, and recover from network and supply chain threats. This will require organizational changes within DoD, increased coordination with the IC, and more cooperation with the Department of Homeland Security and other civilian agencies. It will also require improved relations with contractors, new standards and best practices, changes to acquisition strategy and practice, and initiatives that motivate contractors to see active risk mitigation as a "win." Risk-based security should be viewed as a profit center for the capture of new business rather than a "loss" or an expense

1 The four primary attack vectors in an asymmetric blended operation are supply chain (software, hardware, services), cyber-physical (cyber systems with real-time operating deadlines including weapons systems and industrial control systems), cyber-IT (informational technology), and human domain (witting or unwitting; foreign intelligence service or insider). Most operations use more than one of these vectors to realize an operational effect, moving between them as a function of time as access and opportunity allow. Viewing only cyber-IT as the primary vector affords the adversary a great degree of obfuscation and opportunity in the other three.

harmful to the bottom line. While DoD cannot control all the actions of its numerous information system and supply chain participants, it can lead by example and use its purchasing power and regulatory authority to move companies to work with DoD to enhance security through addressing threat, vulnerabilities, and consequences of its capabilities and adapt to dynamic, constantly changing threats.

Improved cyber and supply chain security requires a combination of actions on the part of the Department and the companies with which it does business. Through the acquisition process, DoD can influence and shape the conduct of its suppliers. It can define requirements to incorporate new security measures, reward superior security measures in the source selection process, include contract terms that impose security obligations, and use contractual oversight to monitor contractor accomplishments. Of course, there are limitations on what DoD can accomplish. DoD is not so large a customer that it can control all parts of its supplier base. DoD has strongest influence over companies with which it contracts directly. Nonetheless, DoD spending is a principal source of business for thousands of companies. The Department can reward the achievement, demonstration, and sustainment of cyber and supply chain security. It will take time to establish workable, fair processes, but these efforts should be given high priority. Where justified by urgent circumstances, the Department should consider use of interim rules to effectuate *Deliver Uncompromised* (DU) in near-term procurements.[2] By adding more security measures to the acquisition toolkit and making better use of those measures, DoD can exercise security leadership through use of its contractual leverage. This issue is elaborated more fully in *Annex I* of this report.

To succeed with *Deliver Uncompromised* requires commitment at the *enterprise* rather than the *element* level—for the Department and for its contractor base. Given the threat environment and its consequences for DoD, this report identifies a number of strategic elements—courses of action (COAs)—to address the cyber and supply chain security challenge. The COAs collectively can form an Implementation or

2 The genealogy of the term "Deliver Uncompromised" began at a 2010 National Counterintelligence Policy Board meeting when Bill Stephens of the Defense Security Service (DSS), along with National Security Agency CI representative Alan Brinsentine, coined the phrase during an informal conversation. Both were concerned that the U.S. government tolerated contract firms that repeatedly delivered compromised capabilities to DoD and the IC. A few months later, the National Counterintelligence Executive Senior Policy Advisor, Mr. Harvey Rishikof, joined in the conversation. The concept was developed at DSS CI and validated by their counterintelligence collection and analysis program largely built upon the rich reporting of suspicious contacts from cleared industry. Further conversations between the DSS CI leadership and affected government and contractor professionals eventually led to a DSS article in the American Intelligence Journal (Vol 29, no 2, 2011), entitled "The T-Factor and Cleared Industry." DSS CI continued to explore the concept until the organization rolled it out as a panel topic at the DSS 2016 Foreign, Ownership, Control and Influence annual meeting. The Undersecretary of Defense for Intelligence then joined with DSS in a contractor-facilitated DU conversation with likely U.S. government and industry stakeholders. The Office of the Secretary of Defense (OSD) and DSS brought this conversation to this MITRE study effort in order to help DoD find a solution to better maintain its technological advantage.

Campaign Plan that could operate along roughly eight lines of effort: Elevate, Educate, Coordinate, Reform, Monitor, Protect, Incentivize, and Assure.

This report examines options that span legislation and regulation, policy and administration, acquisition and oversight, programs and technology. Actions are presented for the near, medium, and long terms—recognizing the need for immediate action coupled with a long-term commitment and strategy. Cyber and supply chain vulnerability extends well beyond DoD, across government and into the private sector. Nonetheless, DoD has potentially decisive influence in this space. Beyond DoD, actions in the legislative domain are critical, as our adversaries are actively exploiting seams and shortcomings in areas such as information sharing, threat detection, and acquisition transparency. Building effective deterrence to asymmetric threats will require time and deliberate planning. The 15 COAs are:

1. Elevate Security as a Primary Metric in DoD Acquisition and Sustainment
2. Form a Whole-of-Government National Supply Chain Intelligence Center (NSIC)
3. Execute a Campaign for Education, Awareness, & Ownership of Risk
4. Identify and Empower a Chain of Command for Supply Chain with Accountability for Security and Integrity to DEPSECDEF
5. Centralize SCRM-TAC with the Industrial Security/CI mission owner under DSS and Extend DSS Authority
6. Increase DoD Leadership Recognition and Awareness of Asymmetric Warfare via Blended Operations
7. Establish Independently Implemented Automated Assessment and Continuous Monitoring of DIB Software
8. Advocate for Litigation Reform and Liability Protection
9. Ensure Supplier Security and Use Contract Terms
10. Extend the 2015 National Defense Authorization Act (NDAA) Section 841 Authorities for "Never Contract with the Enemy"
11. Institute Innovative Protection of DoD System Design and Operational Information
12. Institute Industry-Standard Information Technology (IT) Practices in all Software Developments
13. Require Vulnerability Monitoring, Coordinating, and Sharing across the Supply Chain of Command
14. Advocate for Tax Incentives and Private Insurance Initiatives
15. For Resilience, Employ Failsafe Mechanisms to Backstop Mission Assurance

Deliver Uncompromised

For the long term, DoD should articulate an end-state or strategic endpoint to serve as a "North Star" to guide and measure progress. We believe this initial collection of recommended actions within the *Deliver Uncompromised* framework is a solid foundation for this strategy.

Contents

Understanding the Scope of the Threat

The character of war is changing. Our adversaries no longer have to engage us kinetically; they have shifted their strategy to engage us as a nation *asymmetrically*, exploiting the seams of our democracy, authorities, and morals. They can respond to a kinetic action non-kinetically and often in misattributed ways through *blended operations* that take place through the supply chain, cyber domain, and human elements. They can render our national capability to project power—hard or soft—non-mission ready. They can collapse and even reverse the decision cycle.

We are in an era of adversarial asymmetric warfare for which we have no comprehensive deterrence.

Nation-state adversaries have exploited cyber and supply chain vulnerabilities critical to U.S. security for hostile purposes. These include exfiltration of valuable technical data (a form of industrial espionage); attacks upon control systems used for critical infrastructure, manufacturing, and weapons systems; corruption of quality and assurance across a broad range of product types and categories; and manipulation of software to achieve unauthorized access to connected systems and to degrade the integrity of system operation.

The missions for which the Department of Defense (DoD) are responsible are particularly vulnerable. Adversaries seek to counter areas of U.S. military dominance and to challenge U.S. interests in cyber domains via supply chains upon which our government, our industries, and our populace rely. In this space, traditional boundaries of threat, action, and response are blurred. *We are in an era of adversarial asymmetric warfare for which we have no comprehensive deterrence.* The contemporary threat landscape has not been effectively addressed or deterred in our national security missions, policies, and infrastructures. The response is inadequate within the private sector and across government. The mission readiness of the U.S. military and its ability to project force are at grave risk. Our adversaries have developed and demonstrated capabilities to collect valuable intelligence on defense capabilities, steal intellectual property, initiate offensive action, and respond to provocation in an asymmetric manner. They target military as well as private sector U.S. interests, using means that make attribution problematic. These conditions are without precedent and threaten mission resilience and national security.

Our supply chains are exposed to multiple threat vectors. Supply chains are one of the four primary elements of an adversarial attack via blended operations. Attacks may be mounted against the entire supply chain life cycle from conception to retirement. The supply chain is vulnerable to adversary insertion of counterfeit parts that pass ordinary inspection but fail operationally. Largely through cyber-physical threats, adversaries may introduce malware or exploit latent vulnerabilities in firmware or soft- ware to produce adverse, unintended, and unexpected physical effects on connected

or controlled systems. Supply chains as a service present another critical exploitation vector.

MITRE initially launched this study to help DoD strategically address software supply chain challenges in light of recent legislative branch interest in how "software provenance" was being addressed after the recent Department of Homeland Security Binding Operational Directive 17-1 dealing with Kaspersky Laboratory software. To that end, the report has a pronounced emphasis on addressing software supply chain security. However, the impact of supply chains as a service, hardware, and software on DoD mission readiness and ability to project power requires a strategy that encompasses all aspects beyond just software and within software, beyond just concerns surrounding Kaspersky. To that end, in this report we define supply chain as:

> The system of organizations, people, activities, information, and resources involved from development to delivery of a product or service from a supplier to a customer. Supply chain "activities" or "operations" involve the transformation of raw materials, components, and intellectual property into a product to be delivered to the end customer and necessary coordination and collaboration with suppliers, intermediaries, and third-party service providers.

The resulting COAs should be considered in that light so that the resulting strategy addresses services and hardware in addition to software supply chains.

The result of these attacks is damage to U.S. military readiness, as well as the infrastructure and commercial systems upon which our military relies. Inadequate defense can nullify the value of government and private sector investment and erase expected benefits of new technology. Adversaries will mount cyber and supply chain attacks to slow the progress and deployment of new defense technologies, to compromise the operation and reliability of defense mission and business systems, to replicate what the U.S. technology base has accomplished, and to defeat or deny expected military advantages from U.S. investment in emerging technologies. Stronger, holistic measures to make our networks and supply chains more robust and resilient can deter adversaries by increasing the costs or even reversing the likelihood of adverse effects—reducing the "return on investment" of potential attacks. While one aspect of deterrence is the threat of retorsion or retaliation, a complementary aspect is "gain denial" through measures that deny adversaries confidence in successful attack.

Software vulnerability is a new dimension of security risk, as defined by threat, vulnerability, and consequence, that has received too little recognition. For many if not most DoD systems, software now defines function. Software increasingly determines the boundaries, operation, and risks to systems relied upon by all facets of civil society—consumer-facing, industrial, transportation, energy, healthcare, communications—as well as defense missions and management. Increasingly, functionality is achieved through software. A modern aircraft may have more than 10 million lines of code. The initial Block 1A/1B F-35 had more than 8.3 million lines of code, and later versions

of the aircraft will have more than 20 million lines of code for both operations and support. Combat systems of all types increasingly employ sensors, actuators, and software-activated control devices.

The proliferation of command-driven electronic systems, increasingly connected to sensor-informed networks (even if not initially designed for such linkages), massively expands opportunity for mischief or physical injury achieved through cyber-physical attacks. Software assurance needs to be made a priority for all phases of system acquisition and sustainment. DoD needs to work closely with technical community industrial partners to demonstrate and deploy new methods and measures to identify and respond to software vulnerabilities. Such initiatives acquire new urgency as more and more systems become interdependent and reliant upon the growing instrumentalities of the Internet of Things (IoT).

This report examines options that span legislation and regulation, policy and administration, acquisition and oversight, programs and technology. Actions are presented for the near, medium, and long terms—recognizing the need for immediate action coupled with a long-term commitment and strategy. Cyber and supply chain vulnerability extends well beyond DoD, across government and into the private sector. Nonetheless, DoD has potentially decisive influence in this space. DoD can implement policy and organizational changes, use its acquisition power, and manage the utilization of technology and research and development to address the problems. Beyond DoD, actions in the legislative domain are critical, as our adversaries are actively exploiting seams and shortcomings in areas such as information sharing, threat detection, and acquisition transparency. Building effective deterrence to asymmetric threats will require time and deliberate planning. For the long term, DoD should articulate an end-state or strategic endpoint to serve as a "North Star" to guide and measure progress. We believe this initial collection of recommended courses of action (COAs) within the *Deliver Uncompromised* framework is a solid foundation for this strategy.

Objective: Deliver Uncompromised and Resilient Systems

For the service components that ultimately own the responsibility to execute DoD mission and hence resilience, the primary goal of DoD must be to deliver warfighting capabilities to Operating Forces without their critical information and/or technology being wittingly or unwittingly lost, stolen, denied, degraded, or inappropriately given away or sold. The myriad of systems and capabilities that enable these missions must be resilient and able to respond to anticipated penetrations. The Department's acquisition mechanisms reward cost, schedule, and performance more than integrated risk-management upon which many capabilities rely, especially systems which depend upon complex software. For some years, the Department has pursued a succession of successful "Offset" strategies, focused on innovation in sensors and in network-centric warfare to produce advantages in the delivery and lethality of kinetic firepower. There has been no corresponding strategy, however, for securing that innovation from compromise with an emphasis on mission resiliency. Instead, all too often the Department and its contractors have used a lowest cost set of disparate, unsynchronized security activities and processes that do not match the importance of innovation, information, and technological superiority to our National Security Strategy, National Defense Strategy, and National Military Strategy. The objective of the *Deliver Uncompromised* strategy is to directly address this point, and institute a deliberate, inherent elevation of integrated risk management from concept through retirement, within the DoD and its contracting base, to ensure mission resilience. Choosing not to fight on our terms, our adversaries have embarked upon strategies that exploit the arbitrage of non-coherent defenses and rely on asymmetric capabilities to defeat our technological advances. As evidenced by all-too frequent media reports, our adversaries have had significant success in their strategy. Critical private-sector and military capabilities have been compromised through blended operation attacks, to one degree or another, at various points along the system development life cycle, sometimes prior to delivery, sometimes during sustainment.

State-of-the-Art Security

Independent analysis, respecting the skill and intention of adversaries in asymmetric warfare, should assume that the Department already has experienced systemic compromise, the impact of which may not now be knowable.

Independent analysis, respecting the skill and intention of adversaries in asymmetric warfare, should assume that DoD already has experienced systemic compromise, the impact of which may not now be knowable. The contemporary state of security, unique in the modern era, demands not an "improvement in the same" so much as

a "quantum change" from orthodoxy and established conventions. The response requires a number of strategic actions, some within DoD's span of control, such as leveraging technology and policy, and others, such as legislation or Executive Branch action, requiring the participation and leadership of Congress, the President, and other Executive Branch participants.

For the near term and beyond, the key operational imperative must be to obtain and maintain positive operational control over critical information and technology/capabilities. This imperative extends the benefit of *Deliver Uncompromised* from the acquisition community to the operational community, because maintaining positive operational control is a key element of planning, command assurance, mission execution, and sustainment. Essentially, every element's survival depends upon the ability to release, convey, or transfer information and/or technology under their own initiative and not the unapproved initiative of others. This key imperative may prove to be exceedingly difficult to achieve. DoD and its contractors will have to accept shared responsibility in which all participants take ownership of the challenge and assume a duty of continuing initiative. Absent such an approach, as a nation we risk dilution, or loss, of strategic and tactical advantages.

Too often the focus of government efforts to improve contractor cyber measures is upon perimeter defense, with security professionals assigned principal responsibility. The established presence of Advanced Persistent Threats (APTs) calls into question the operating premise of perimeter security. Counterintelligence personnel need to work with security professionals to inform enterprise actions with an understanding of adversary targets, methods, and priorities.[3]

Today our adversaries may have a better understanding of our strategic vulnerabilities than do we. This includes vulnerabilities introduced via networks or through the supply chain. This is because of poor/inadequate intelligence on such threats, excessive compartmentation that precludes effective sharing of such threat information, lack of prioritization, and widespread availability of information in the public domain. Combined with the inherent vulnerabilities of the natural seams of our democracy,

3 Experience has shown that external sensors for detecting network penetration do not reveal all attempts at penetrations or detect unauthorized outflow that results from APTs. In blended operations, adversaries may avoid the network perimeter and instead use tactics to attack supply chain hardware, software and services. George Patton's observation applies here for how France's Maginot Line, a static defense against German invasion, failed miserably. "Fixed fortifications are monuments to man's stupidity. If mountain ranges and oceans can be overcome, anything made by man can be overcome." The threat environment requires the United States to adopt a counterintelligence mindset to replace our legacy security mindset when securing the defense industrial base. Our adversaries' great success against static defenses should be evidence enough that we need to make this change. To win in the Information Age where the advantage is to the attacker and not the defender, our new frame of reference should be: 1) no defensive perimeter wall is inviolate; 2) every wall has been penetrated or is susceptible to successful penetration by determined actors; and 3) the absence of evidence our security wall has been breached does not constitute evidence there has been no penetration.

this gives our adversaries a significant advantage to which we are just beginning to respond.

The 2018 National Defense Strategy recognizes the degradation of our force projection capability across all domains and specifically calls for the investment of resilient capabilities:

> "Investments will prioritize ground, air, sea and space forces that can deploy, survive, operate, maneuver and regenerate in all domains while under attack. Transitioning from large, centralized, unhardened infrastructure to smaller, dispersed, resilient, adaptive basing that include active and passive defenses will also be prioritized." Likewise, "...New commercial technology will change society and, ultimately, the character of war. The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed. Maintaining the Department's technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base...".

The recommended measures in this study are intended to serve as a foundation which directly supports this strategy.

Structural Challenges

There are fundamental structural challenges facing the Department. If not resolved, these barriers will undermine our ability to *Deliver Uncompromised*. Major challenges to consider are:

1. Overreliance on "trust," in dealing with contractors, vendors, and service providers, has encouraged a *compliance-oriented* approach to security—doing just enough to meet the "minimum" while doubting that sufficiency will ever be evaluated. This approach must change fundamentally so that enterprises are incentivized to find and solve any issue that might place a program at risk or expose systems to vulnerabilities. At the same time, industry needs the means to assess and validate their countermeasure accomplishments. We offer suggestions on how to establish an independent, expert intermediary that industry will trust to develop security metrics and necessary processes for review and assessment.
2. Solving the security issues facing DoD requires increased *counterintelligence* (CI) participation. A *security* community that largely operates to show compliance with established rules may be uninformed of evolving threats and therefore unable to adapt to the agile strategies and asymmetric techniques of adversaries. From Defense Security Service (DSS) reports and supporting documentation by the National Counterintelligence and Security Center (NCSC), as well as

Federal Bureau of Investigation (FBI) field office activities, there are lessons to be learned from the resources that are actively engaged in CI activities. Protection of DoD interests calls for Department leadership, as well as industry, to be kept alert and informed, by DSS, the FBI, and other entities, about the quiet attacks constantly being launched against DoD interests. This is why education and ownership of the problem are so important—and why expanding the resources and authority of DSS is vital.

3. There is no single DoD organization vested with lead responsibility for threats and risks to the defense industrial base (DIB), despite the fact that most major exploitations by adversaries are directed against and occur within the DIB. DoD should consider the DIB assets on a "whole of enterprise" basis, inclusive of assets beyond information and data, and shift from protecting *facilities* to protecting *assets*. Similarly, DoD's contract measures, and accompanying oversight, should evolve from safeguarding *information* and *information systems* to include safeguarding *operations* and enterprise *capabilities*. In this vein, the Department should address its interface with contractors for security practices, so that companies deal with trained resources and avoid inconsistent interpretations and instructions.

4. There has long been widespread recognition that "reform" of the existing acquisition process is needed to address typically over complex, behind schedule, and over budget acquisitions. However, given the changing character of war and our adversaries' asymmetric strategies, these processes, along with how we have maintained and sustained our capabilities, have also resulted in highly compromised systems despite the consumption of huge technical and financial resources, leaving the Department's mission readiness at risk. This fact must drive true reform of the acquisition process. The Vice Chiefs and the Vice Chair, who are ultimately responsible for the operational readiness for their Services, should create and maintain a strong and accountable chain of command for cyber defenses, supply chain security, and digital integrity, and themselves be held accountable. Accountability for integrity and mission readiness must be blended across the acquisition, operations, and sustainment communities, with a clear chain of command directly to the Secretary of Defense (SECDEF) through the Deputy Secretary of Defense (DEPSECDEF).

5. DoD (among other federal departments and agencies) has yet to communicate clearly with sufficient emphasis the importance of security and integrity. This failure is reflected in the recently released *Federal Cybersecurity Risk Determination Report and Action Plan* (May 2018). Across the entire range of enterprise, business, and weapons systems, the Department will benefit from a clear leadership statement and direction that shifts priorities and reduces exposure to compromised delivery. At the national level, the Office of Management and Budget's (OMB) Memorandum M16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," dated Oct. 30, 2015, included

directions to the heads of executive departments and agencies that still merit attention today. Agencies were directed to prioritize identification and protection of high-value information and assets, improve ability to timely detect and rapidly respond to cyber incidents, prepare for rapid recovery from incidents when they occur, recruit and retain the most highly qualified cybersecurity workforce, and make efficient and effective acquisition and deployment of both existing and emerging technology.

Contractual Leverage

Ultimately, improved cyber and supply chain security requires a combination of actions on the part of the Department and the companies with which it does business. Through the acquisition process, DoD can influence and shape the conduct of its suppliers. It can define requirements to incorporate new security measures, reward superior security measures in the source selection process, include contract terms that impose security obligations, and use contractual oversight to monitor contractor accomplishments. There are limitations upon what DoD can accomplish. DoD is not so large a customer that it can control all parts of the supplier base upon which it draws. And DoD has strongest influence over companies (large and small) with which it contracts directly. Nonetheless, DoD spending is a principal source of business for thousands of companies. The Department can reward the achievement, demonstration, and sustainment of cyber and supply chain security. It will take time to establish workable, fair processes, but these efforts should be given high priority. Where justified by urgent circumstances, the Department should consider use of interim rules to effectuate DU in near-term procurements. Adding more security measures to the "acquisition toolkit," and making better use of those measures, are ways DoD can exercise security leadership through use of its contractual leverage. This issue is elaborated more fully in *Annex I* of this report.

Courses of Action (COAs)

To succeed with *Deliver Uncompromised* requires commitment at the *enterprise* rather than the *element* level—for the Department and for its contractor base. Given the threat environment and its consequences for DoD, this report identifies a number of strategic elements—courses of action (COAs)—to address the cyber and supply chain security challenge. We classify actions into short term (ST), medium term (MT), and long term (LT), based on how quickly and urgently the Department should *initiate* action. The COAs are listed here and described in more detail further in the report:

Deliver Uncompromised

	COAs	
1	Elevate Security as a Primary Metric in DoD Acquisition and Sustainment -ST	It is vital to Deliver Uncompromised that security have equal status to cost, schedule and performance. Revise DoD 5000.02 and Defense Acquisition Guidance to make security the "4th Pillar" of acquisition planning, equal in emphasis to cost, schedule and performance. Utilize acquisition tools and contract leverage and reinforce the objective of Deliver Uncompromised through the use of positive and negative incentives.
2	Form a Whole of Government National Supply Chain Intelligence Center (NSIC) -ST	Follow the example of the National Counterterrorism Center (NCTC) to integrate Title 10 and Title 50 "all source" supply chain threat intelligence and strategic warnings. Led by NCSC and heavily supported by an expanded DSS capability, extend out to include FBI, DHS, and other civilian agencies and share warnings and actions with contractors.
3	Execute a Campaign for Education, Awareness, & Ownership of Risk -ST	Educate all program and supply chain participants on the goals of Deliver Uncompromised and the breadth and nature of cyber and supply chain threats. Build and maintain training programs for DoD personnel, including measures to improve the expertise of persons assigned contractor oversight responsibilities.
4	Identify and Empower a Chain of Command for Supply Chain with Accountability for Security and Integrity to DEPSECDEF -ST	The Service Vice Chiefs are ultimately responsible for the operational readiness of acquired capabilities under their command and should require that acquisitions are conducted in a manner that values system integrity and mission resilience to Deliver Uncompromised. Cross-Service vulnerabilities and opportunities for effective threat response across the Department can be served by the Vice Chairman, Joint Staff, and possibly an accountable Supply Chain Security Executive. Organize resources to support this chain of command and hold them accountable to the DEPSECDEF for successful implementation.
5	Centralize SCRM-TAC with the Industrial Security/CI mission owner under DSS and Extend DSS Authority -ST	The Supply Chain Risk Management – Threat Analysis Cell (SCRM-TAC) is isolated from industry information sources and from operational elements supporting industry that are vital to structured SCRM analytic production. DSS has access to DIB information on classified contracts and has operational elements directly supporting industry. Consolidation could significantly improve DoD's cyber and supply chain strategic warning. This consolidation would result in a well-staffed and organized body of independent analysts, well trained in structured analytical techniques, which then could be positioned to help the program acquisition community directly address risk to programs as a function of not only threat, but system vulnerabilities and potential consequences.

		COAs
6	Increase DoD Leadership Recognition and Awareness of Asymmetric Warfare via Blended Operations -ST	Ensure that the entire DoD leadership is aware of the goal of DU and that adversaries seek not to engage the United States kinetically but instead are using cyber and supply chain attacks to exploit and degrade key national security capabilities. Educate leadership in DoD to "own" the problem and make detection and defense against these threats a natural part of everyday duties.
7	Establish Independently Implemented Automated Assessment and Continuous Monitoring of DIB Software -MT	Develop, validate, and exploit technical methods to assess and validate software security and integrity. Evaluate whether to require suppliers to use independent, continuous monitoring to detect software nonconformity and developmental abnormalities and to automate patching and recovery.
8	Advocate for Litigation Reform and Liability Protection -MT	Reduce liability exposure to encourage prompt contractor reporting of cyber and supply chain events. Encourage investment in integrity measures by providing new liability protection (e.g., extend SAFETY Act to cyber and supply chain).
9	Ensure Supplier Security and Use Contract Terms -MT	In new acquisitions, treat data security, product integrity, and supply chain assurance measures as competitive discriminators, and make end-product mission resilience a key contract award metric. Consider use of interim rules to expedite the availability of these tools for critical near-term procurements. Structure acquisitions so contractors have a profit motive to enhance security; establish standards and methods to enable contractors to earn and retain levels of independently verified established resilience. Use an independent Security Integrity Score (SIS), much like a "Moody's" rating in the financial world, which rates each potential contractor in a unified manner by an independent, unbiased third party.
10	Extend the 2015 National Defense Authorization Act (NDAA) Section 841 Authorities for "Never Contract with the Enemy" -MT	Extend existing authority to protect DoD against risks of contracting with entities under control of adversaries; provide for expedited action in high-threat situations. Empower the Supply Chain Executive to act on NSIC advice in conjunction with enforced responsibilities within the Combatant Commands against awards to sources of established assurance risk.

		COAs
11	Institute Innovative Protection of DoD System Design and Operational Information -MT	Minimize and obscure the dissemination of system design information, even within the design and build teams, but especially with vendors and contractors. Share what information needs to be shared only as long as needed and no more; utilize technical measures to protect data access and use rights at the file level.
12	Institute Industry Standard Information Technology (IT) Practices in all Software Developments -MT	Address the full span of software vulnerability through measures in acquisition and operations through full life cycle continuous security and risk reduction practices from concept through retirement. Determine where and for what programs or missions it is recommended or necessary to require submission of a Software Bill of Materials (SBOM) and require a documented Secure Software Design Life Cycle (SSDL).
13	Require Vulnerability Monitoring, Coordinating, and Sharing across the Supply Chain of Command -MT	The NSIC should serve as the focal point to aggregate vulnerability information across all sources of public and private source information, including Defense intelligence and other IC content. Each Service component in both acquisition and sustainment should look for and coordinate information sharing among themselves and with designated software vulnerability information sharing mechanisms such as Common Vulnerabilities and Exposures (CVE), Information Sharing and Analysis Organizations (ISAOs), United States Computer Emergency Readiness Team (US-CERT), National Telecommunications and Information Administration (NTIA), and Department of Justice (DOJ).
14	Advocate for Tax Incentives and Private Insurance Initiatives -LT	Work with Congress to provide tax incentives for contractors that invest in cyber and supply chain assurance, which is independently and routinely evaluated. Promote contractor use of cyber and supply chain insurance with government excess liability coverage.
15	For Resilience, Employ Failsafe Mechanisms to Backstop Mission Assurance -LT	For every critical function for which the consequence of an attack is denial of mission execution, develop means to execute the mission in a degraded state while under attack. Utilize "uncorrelated means" of accomplishing the missions in system and subsystem designs and diversity at the component, Service, or enterprise levels.

COA Details

1. Elevate Security as a Primary Metric in DoD Acquisition and Sustainment (ST).

Acquisition today is driven to meet cost, schedule, and performance objectives. Absence of incentives for security contributes to widespread compromised systems. Currently, the misalignment of risk and reward during acquisition results in systemic risks being transferred to the operational and sustainment communities without accountability. DoD must shift from measuring program progress primarily by financial considerations to a metric of durable operational readiness of acquired systems. Planning must account for the true cost of ownership of capabilities. Existing contract authorities should be leveraged to require demonstration of system integrity and mission assurance to be a deliverable, to the best extent reasonably possible; software security and system resilience should be Key Performance Parameters for contract execution. Methods of providing continuous monitoring of system integrity and having alternate means of executing mission function through system design and engineering (at the subsystem, system, and enterprise levels) and through prepared operational strategies are essential to increasing resilience and "fight through" capability.

As we introduce new and more secure processes to the private and public sectors, increased cost is to be expected. Absent adjustment, cost factors too often drive decision making away from the desired security outcome. When viewed from the asymmetric threat perspective, this is an undesirable outcome that can be avoided only through high-level priority, policy, and accountability changes. Part of the new strategy must be to transform security concerns from a cost center to a profit center. Additional funding will be needed to avoid the outcome that treating security as a "4th pillar" will produce undesirable compromises to cost, schedule, or performance. Products free of compromise represent more value than compromised products and have reduced total cost of ownership.

Means of accomplishing this objective are further discussed in this report. One important strategy is to use acquisition authority to adjust the expectations of private sector contracting partners. Few DIB participants disagree that a better job can be done with security and integrity. Many, however, are unsure how to "benchmark" what they have accomplished so as to manage their own progress and, if asked, demonstrate to DoD, or to primes or higher tier contractors, that they are worthy of trust.

To realize security as the "4th pillar" requires that the degree of risk a current or potential contractor presents to the government be continuously measured and monitored. We see this evaluation taking place in three dimensions: measured by the government on currently performing contractors as a future performance indicator; measured by an independent not-for-profit or federally funded research and development

center (FFRDC) much like a "Moody's" score and made publicly available; measured privately by the contractor via the private sector to monitor their operational risk.

The commercial sector is currently developing various services to address the last measurement technique. In investigating the second "Moody's"-like scoring, we have received a positive response, within the Department and DIB community, to creation of an independent, expert resource to create and operate a security scoring mechanism. Conceptually, SIS could be used in bidder qualification and in the selection and award of contracts. DoD and industry should partner to create an independently administered entity, perhaps a not-for-profit 501(c)(3) organization, to create standards and processes for risk-based evaluation and scoring of contractors, perhaps separating contractors into "tiers" of accomplishment, and accompanied by commitments to continuous monitoring, reporting, and self-improvement. Use of SIS would be phased in, figuring initially into acquisition decisions for Major Defense Acquisition Programs (MDAPs) and other, selected high-impact programs. Over time, as government and industry become confident in the value of SIS, they can become an important part of the acquisition process for more programs and for many levels of the supply chain. Receipt of SIS credentials could be valuable in qualification for commercial supply chain participation as well.

All too often today, DIB contractors are reluctant to price added integrity and integrated risk management into their bids because the U.S. government rarely requires it in the Request for Proposal (RFP), and they fear losing the contract where higher cost may be a decisive negative discriminator. Adding security credentials into the mix by crediting SIS as earned should motivate contractors to make the needed investments and to secure development environments, moving security from the loss column to the profit column.

The historical emphasis on "cost, schedule, and performance" is a fundamental driver for actions of DoD as well as the DIB. The DoD requirements process has not put security and integrity on an equal footing, with the result that the costs of assurance work against the usual program metrics. This approach works against the integrity of weapon platforms in today's world of diverse and severe cyber and supply chain threats. For all aspects of the system development life cycle, and throughout operation, sustainment, and system disposition, security must have higher priority. Dispersed, agile, and evolving threats require continuous commitment from both government and industry participants. Special attention is required for software security—an area of great exposure but given relatively low priority at present.

Even after increasing the importance of security across the acquisition process, there are other areas DoD needs to address for continuous improvement over a longer term:

- The Department already invests in new technologies that can be applied to identify and mitigate cyber and supply chain threats in the near term, mid-term, and long term. Where breakthrough technologies are found, they should be rapidly

exploited. The Department already is expanding use of non-procurement "Other Transaction Agreements" (OTAs) under 10 USC §2371b. To encourage innovation by its established and dedicated contractors, the Department should be able to make OTA awards to both "nontraditional" and "traditional" defense contractors. Beyond application to prototype projects, DoD may need clarified and enhanced legislative authority for transition from prototype to production and deployment, where justified by national security considerations.

- Constraints remain in the ordinary application of today's "full and fair competition" rules to DoD acquisition at all phases of the system life cycle. Further study is needed to remove barriers to rapid, secure accomplishment of national security goals, while recognizing that competitive opportunity encourages industry partici- pation and innovation. In the same vein, the Department should consider whether pending "acquisition reform" initiatives (such as the Section 809 Commission) give sufficient weight to security. As it considers the 809 Commission recommen- dations, the Department must assess the tension between current and planned reform actions and the full scope of the asymmetric threat and response.
- DoD needs to retain the trust of its contractors, who will not invest as needed in security (or in new technologies) without assurance of opportunity for return through a fair competitive process. Program budgets must incorporate funds sufficient for higher levels of security. Product integrity, data security, and supply chain assurance should become key contract award criteria. This will remove today's security disincentive, as contractors now risk the award should they include costs that ensure delivery of uncompromised capabilities. In the competitive source selection process, DoD should incentivize bidders to make demonstrable and independently verifiable improvements to the protection of their system development and delivery processes and to sustained security over system life.
- "Transparency" and "open government" have policy benefits but expose massive amounts of exploitable information to adversaries, contributing to their knowledge base without counterpart exposure to the United States. This must stop. For high-impact programs and critical technologies, and in areas where known cyber and supply chain risk is present, the Department may need authority to obfuscate program and procurement information—and it will need corresponding capabilities from its private sector partners and their suppliers.
- DoD has reasons to seek more knowledge of contractor technologies, more data about as-built configurations, and more insight into supplier selection, pedigree, and provenance. These interests must be balanced with recognition that intellectual property (IP) is a critically important asset to many contractors, and DoD must assure its suppliers it can protect their IP, where demanded and delivered, and that contractors will retain the ability to exploit the IP of their innovations. DoD should always be mindful that its contractors must have a positive business case before they incur new costs and responsibility for software assurance or other security improvements.

For budgeting and planning, the Department needs to address the financial consequence of losing or utilizing a compromised critical system—including the ultimate cost of a failed mission for which the capability was developed in the first place. Likewise, much of the technological advantage the United States has enjoyed is constantly eroded due to adversary theft of key designs and technologies. (There are numerous examples of nearly identical adversary capabilities that our enemies have fielded as a result of compromised acquisitions.) To provide the requisite system security or confidence—from the outset rather than as a midlife correction or enhancement—realistic resource assessments should be factored into the expected acquisition and sustainment budgets. As shown in Figure 1, the up-front costs of a representative acquisition appear significantly different for a supply chain adequately protected from inception. The apparent cost differential, however, is significantly smaller for the protected acquisition when compared to the higher total cost of ownership experienced where failure to secure the supply chain initially delivers compromised products requiring expensive attempts at correction later in program life.

Once an exploited vulnerability is discovered, a new acquisition effort will be required to replace or re-engineer a deployed system. If the process is not protected, it may be

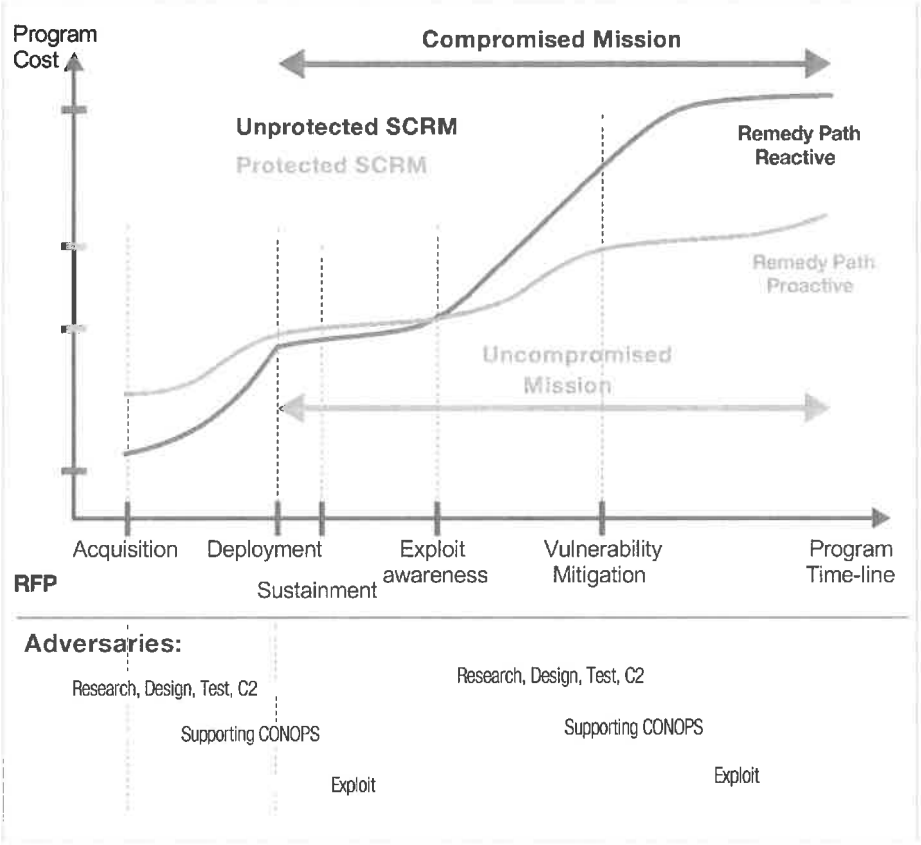


Figure 1: Cost framework for SCRM: Total cost of ownership implications

attacked again. Most serious in this entire paradigm is the loss of the ability to ensure that the mission for which the system is designed can be successfully conducted, and/or the loss of overmatch of the U.S. capability over the adversary.

2. Form a Whole-of-Government National Supply Chain Intelligence Center (NSIC) (ST).

Supply chain threats include but extend beyond the DIB. A whole-of-government (WOG) response first includes DoD and the IC with likely leadership from the National Counterintelligence Security Center (NCSC). This strategy then should then be extended to FBI, DHS, and other civilian agencies. DoD should endorse and support a national joint, inter-agency entity—the NSIC—that can aggregate all-source data, both classified and unclassified, cyber and non-cyber, and share it with at-risk operators and industrial partners. The NSIC should follow the NCTC model functionally. The NSIC would be jointly governed, likely reporting to the Director of National Intelligence (DNI), the Under Secretary of Defense for Intelligence (USD[I]), and the NCSC. The goal of the NSIC would be to support the delivery to Operating Forces of warfighting capabilities that are uncompromised and resilient (i.e., without their being wittingly or unwittingly lost, stolen, sold, inappropriately given away, degraded, or denied) through the use of all-source intelligence and warning. In the wake of the 9/11 events, President Bush worked with Congress to create the NCTC to enable the responsible exercise of new investigative and analytical authorities and information collection, consolidate data, facilitate information sharing, and provide national, state, and local warning within and across various public-sector entities. Its stated purpose is to "lead and integrate the national counterterrorism (CT) effort by fusing foreign and domestic CT information, providing terrorism analysis, sharing information with partners across the CT enterprise, and driving whole-of-government action to secure our national CT objectives." Creation of the NSIC would be a similar initiative, drawing from experience and lessons learned over more than a decade of NCTC operations. From the DoD perspective, this could be partially realized by centralizing SCRM-TAC with the Industrial Security/CI mission owner under DSS lead.

With new authorities supported by policy and legislative changes, the NSIC would be able to share intelligence-based strategic warning among all DoD components and mission owners and, eventually, with all U.S. government (USG) department and agencies. This would contribute to a national resource for threat collection and analysis that produces actionable intelligence and measures that can be utilized across the WOG at the unclassified level. This integrated resource would develop and operate technologies for threat detection, artificial intelligence, and data analytics, enabling analysts to "connect the dots" among subtle and disparate data from a wide variety of sources. Risk assessments require an understanding of system vulnerabilities and their consequences across the supply chain cycle, as shown in Figure 2.

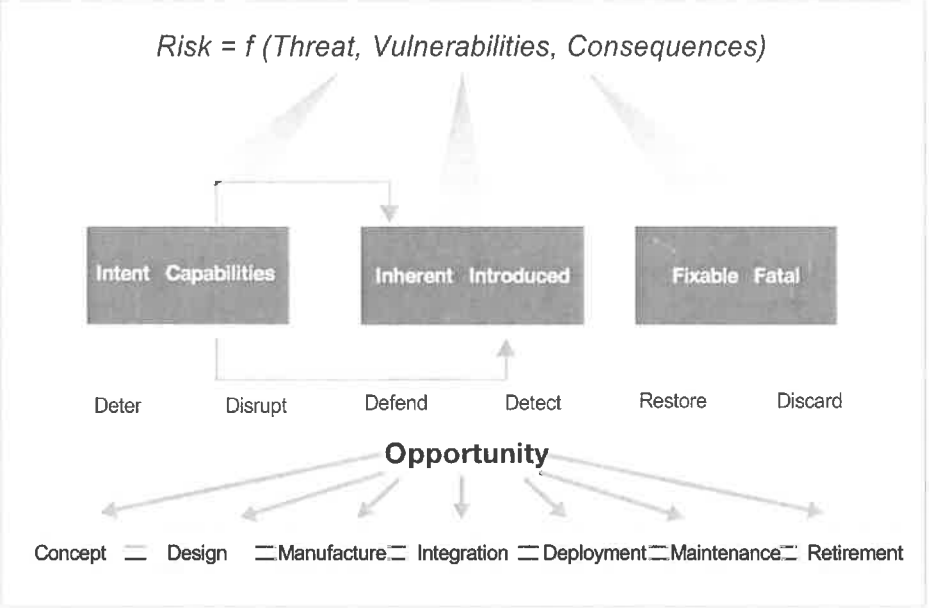


Figure 2: Supply chain risk assessment and integrated response

Risk assessment is crucial to supply chain defense and assurance of system integrity. Knowing the threat is the essential first function of successful risk assessment and supply chain defense. Existing stovepipes of legacy sectoral assignments hinder fully informed actions. Imperfect or incomplete intelligence dilutes the value of assessments and recommended actions while increasing the probability of a missed detection or false alarm. The NSIC will generate high-value threat assessments and be positioned, through joint interagency interactions, to help its component members develop measures of risk based on their specific vulnerabilities and mission failure consequences. It can combine all-source government intelligence, data from civilian agencies, and private sector reports.

As the center of excellence for supply chain strategic warning and risk assessment, the NSIC will be expert in knowing potential system vulnerabilities (inherent or introduced) if populated with representatives from the program and system engineering communities. The NSIC should be staffed with and led by trained analysts and subject matter experts who understand both the engineering technical characteristics of a potential exploitation as well as potential tactics, techniques, and procedures (TTPs) an adversary may use. Multiple, diverse stakeholders from across the development and acquisition community can use warnings produced by the NSIC. Consequences can be averted or mitigated by timely warning coupled with expert advice on response and recovery, as shown in Figure 3.

Attention must be directed to communicating strategic warnings (and action recommendations) to industry, as it is frequently the target and is best able to protect,

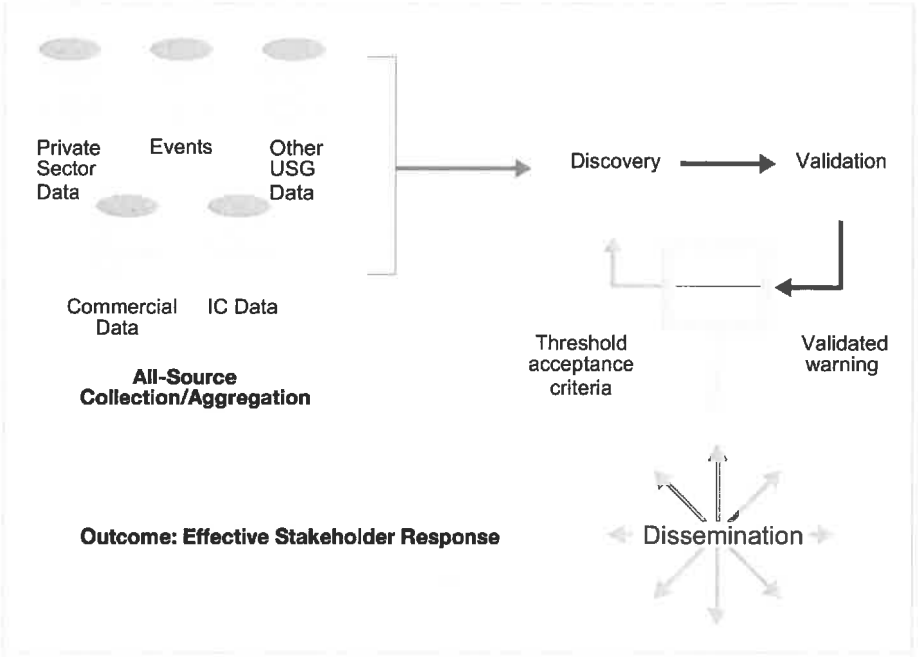


Figure 3: Distribution of source data, validation and warning, and action

detect, respond, and recover. Today, the distribution of threat information to industry—if it occurs at all—is too slow and too cumbersome. In an information age, means are needed to communicate electronically to industry. Methods must be established to share threat information and recommendations with companies who are not cleared contractors. It is difficult to translate from classified threat data into unclassified warning, but this is a responsibility that should be assigned to the NSIC. Informing only cleared industry is not satisfactory—it leaves the great majority of companies in the DIB uninformed and exposed.

This concept can also significantly reduce duplicative government purchasing of commercial data sources.

3 Execute a Campaign for Education, Awareness, and Ownership of Supply Chain and Digital Risk (ST).

Program executives and the acquisition workforce must be better informed, educated, and trained. The entire acquisition and sustainment community must become aware of the expanse of the asymmetric threat we face. As a matter of duty, supporting personnel must understand and "own" the problem—namely a lack of appreciation of how the new threat environment has made the supply chain a vector of attack and that this vulnerability continues for the entire supply chain cycle. As stated at

the outset, the supply chain is exposed to multiple threat vectors and categories. As shown by the recent experience with Kaspersky Labs anti-virus software, our software supply chains are being exploited, potentially on a massive scale, that could produce a host of nefarious outcomes. Supply chain risks extend beyond the subject of cybersecurity that often dominates the attention of Department leadership. Risks exist through the entire supply chain cycle and are not limited to networks and information systems. Deliberate insertion of non-conforming parts can sabotage mission capability. The firmware or software in electronic parts can be the subject of corruption or subversion. Adversaries, unfortunately, have many choices among attack surfaces to produce effects adverse to defense planning and mission execution.

New comprehensive curriculums on supply chain risk and asymmetric adversary intent should be readily available at the Department (e.g., Defense Acquisition University, National Defense University, National Intelligence University, etc.) and Component levels to members of the acquisition, operations, and sustainment communities.

The human factor contributes to supply chain risk. Individuals can enable, even engineer, hardware and software attacks. Insider threats remain among the most important causes of successful compromise. They can arise by design and intention, where an insider is untrustworthy, subject to foreign control or influence, or otherwise suborned, through means such as a social engineering attack. The same outcome can result from imprudent or uninformed actions without any hostile intent, by persons who lack sufficient training or who are given unmonitored or overbroad access to or authority over connected systems. Best practices for supply chain protection, in government and industry, call for improved training and better monitoring to detect, limit, or prevent insider-caused events.

Too often, within DoD and industry, senior executives pay insufficient attention to supply chain assurance—and too little investment of money or other resources—because they lack sufficient understanding of the problem and the hidden operational risks they incur. The awareness campaign recommended here is not a one-time or static exercise. Training has to evolve to keep pace with the intense rate of change in this threat/response landscape.

4. Identify and Empower a Chain of Command for Supply Chain with Accountability for Integrity to DEPSECDEF (ST).

How systems are engineered and designed in the future should be a fundamental focus for the Defense Research and Engineering (R&E) and Acquisition and Sustainment (A&S) communities. How capabilities are acquired and operated in a secure manner ultimately lies with those charged to organize, train, equip, and command—the Components. This needs to be reinforced. Consequently, the Service Vice Chief would be the official best positioned to reconcile inputs from Acquisition (cost, schedule and performance) and from the IC and CI (Security) through their development and approval of requirements and acceptance of delivered capabilities. Since supply chain security is an overarching domain—affecting requirements, acquisition, operations, and sustainment—the Service Component Vice Chiefs should own the responsibility to ensure that the acquisitions under their command and for their operations are conducted in a manner that values system integrity and mission assurance to *Deliver Uncompromised*. Cross-Service vulnerabilities and opportunities for effective threat response across the Department can be served by the Vice Chairman, Joint Staff, and possibly an accountable Supply Chain Integrity Executive within the Office of the Secretary of Defense (OSD). These resources should be organized to support this chain of command and be held accountable at the Vice Chairman and the Executive levels to the DEPSECDEF for successful implementation with authorities that span the Department.

Breadth of the Supply Chain Threat

Counterintelligence and security should not be subordinate to business and engineering professionals. The supply chain threat is larger than information and communications technology and extends beyond network-delivered cyber attacks upon information and information systems.

This authority should be coupled with personal accountability. The function affects all Military Departments as well as the fourth estate supporting agencies. Just as the corporate world is now standing up Vice Presidents for Supply Chain, and DNI/NCSC has a Supply Chain Directorate, DoD's supply chain responsibilities should be vested in these single individuals and offices with expanded authority and strong lines of interaction across the Department. Counterintelligence and security should not be subordinate to business and engineering professionals. The supply chain threat is larger than information and communications technology and extends beyond network-delivered cyber-attacks upon information and information systems. Accordingly, if system and supply chain integrity is viewed as its own mission, there are many contributing functions, among them Chief Intelligence Officer and cyber, CI and Defense Procurement and Acquisition Policy (DPAP), systems engineering and industrial base, etc. Considered as a whole, the potential function of a DoD supply chain executive reaches to

issues of technology base and national assets, such as foundries and field-programmable gate array (FPGA) assurance and supply, and the advancement of specialized assurance technologies such as automated software verification and emerging methods of authentication and measurement to protect against threat vectors from the IoT. Consolidated authority is needed for effective coordination among many contributing functions and to enable DoD *leadership* to make *strategic* decisions on approach, investment, and execution of assurance measures and to interact, coordinate, and collaborate across the WOG in a more consistent manner. It would ensure proper, accountable representations across the WOG as the nation begins to seriously deal with the supply chain security issue.

5. Centralize SCRM-TAC under DSS and Extend DSS Authority (ST).

SCRM-TAC, at present, is not well linked to USG and DoD assets performing operational intelligence, counterintelligence, security, and law enforcement prosecution. Although DoD, pursuant to instructions 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), and Committee on National Security Systems Directive 505, Supply Chain Risk Management, has worked with SCRM-TAC, Joint Acquisition and Protection Cell, and Joint Federated Assurance Center to produce a TSN Mitigation Playbook, vulnerabilities have continued to plague the process. SCRM-TAC focuses on portions of the *intent* and *capability* of adversaries, but not Component capability *vulnerabilities* and *consequences*, which are the domain of the acquisition and sustainment communities and elements of "DSS In Transition" currently being stood up. SCRM-TAC also is isolated from industry information sources.

DSS, in contrast, has CI operators in the field, and access to DIB information on classified contracts. The capability of DSS would be more robust and scalable if SCRM-TAC were to report to DSS. In this context, "report" should be understood to mean both administrative control and operational control. Production of supply chain intelligence would be enriched and accelerated by this change and further enhanced by combining these sources with content from the FBI and other authorities as needed. These would be initial steps for the Department's participation in a wider community-wide strategic warning capability, as is the intent of NSIC as described above. A consolidated, well-staffed and organized body of analysts well trained in structured analytical techniques could then be positioned to help program acquisition and sustainment to actually address *risk* to the program as a function of not only threat, but system vulnerabilities and potential consequences.

Elements of the acquisition community within DoD, however, are attempting to use SCRM-TAC as a clearinghouse on risk—a function that cannot be provided in the construct as described above. There are many elements and definitions of risk, and DoD should standardize on its own Defense Science Board and NCSC definition, as

illustrated in Figure 2 above. In some instances, SCRM-TAC is asked to provide the "risk" of a program utilizing specific components; in others, the risk of an entire system design. In nearly all instances, SCRM-TAC is utilized relatively late in the process, well after major procurement and design decisions have been made, and lacks sufficient information to conduct such assessments. At the program acquisition planning level, there seems to be less than recommended receptivity for strategic warning, especially when related to enterprise-wide threats. We have made several recommendations to specifically address these problems and approach supply chain security with threat analysis, information sharing, and intelligence management functions that would holistically address the challenge and mitigate risk. Although a daunting challenge, this report concludes that it is vital to recognize and address supply chain threats early in the acquisition planning rather than react later in the program cycle and attempt remediation after systems are built and deployed.

6. Increase DoD Leadership Recognition and Awareness of Asymmetric Warfare via Blended Operations (ST).

Our adversaries have demonstrated they wish to engage us *not* kinetically but rather asymmetrically. The landscape of potential non-kinetic adversary attacks is broad indeed. The United States lacks a comprehensive deterrence against these actions. We worry and debate over the possibility of a lawsuit by a contractor or supplier who is intentionally jeopardizing mission assurance while China openly discusses "lawfare" as a *strategy*. All levels of DoD leadership must fully understand the adversary's strategic intent to act through *all of* the supply chain (hardware, software, and service), cyber IT, cyber-physical, and the human element (witting or unwitting), and adjust the Department's response and posture accordingly.

As with other military domains (air, sea, land, and cyber), asymmetric warfare is, among other characteristics, complex and destructive, with offensive and defensive capabilities and a commitment to action (strategies and tactics). National leadership must recognize that we are currently in a state of war within all of these domains via asymmetric actions. The ability to take a whole-of-government or whole-of-society approach to combat an adversary's attack must take on the same level of investment, planning, and implementation we would exercise for a more conventional attack on our homeland and allies. A key part of the strategy is to reform our acquisition policies and authorities to combat an adversarial manipulation of the supply chain and work with the private sector.

The impact of this insidious asymmetric warfare against the United States has gone largely unrecognized. Some refer to this domain as conflict in the "gray zone" because of its comparative absence of visibility and the continuing challenge to attribution to responsible actors. Awareness of the true complexity of the asymmetric threat is distorted by the very nature of the technical and operational approaches our adversaries are employing in their attacks. Our response has been stunted because

of the lack of public awareness and understanding of adversaries' intentions, capabilities, or hostile acts.

Most nation-states have a full complement of technologies available to achieve their asymmetric strategies and goals. The development of effective approaches to take advantage of inherent vulnerabilities in complex systems is well within their capabilities and the access to our systems they enjoy through our supply chains. Likewise, through reverse engineering of complex systems, nation-states are capable of introducing or inserting vulnerabilities for exploitation.

This full-spectrum threat is not only capable of developing technical products, but is coupled with the requisite operational tradecraft, training, access development, and resources to mount an effective attack. All levels of DoD leadership must fully understand the adversary's strategic intent to act through blended operations.

Even the relatively unsophisticated actors, with limited or incomplete knowledge of our systems, can develop capabilities that have a profound impact on our offensive and defensive capabilities and infrastructures; to deny us the ability to effectively utilize them to achieve our tactical and strategic objectives. These capabilities are often available through third-party venues that leverage nation-state investments, often at low cost.

A significant shortfall in our defense is the lack of visibility to identify our adversaries' signatures or implementation across multiple domains and critical infrastructures. Indeed, misattribution of their actions is an important part of their strategy. In part this is due to the segmentation of responsibility we have imposed on ourselves for decades. Today, responsibility for risk to DoD capabilities is dispersed across departments and agencies and among many DoD Components and entities. The result is that leadership views their roles and responsibilities, with respect to security and acquisition integrity, through many different lenses. Each lens provides a limited view of the complete landscape in which we procure and maintain our weapon systems, exercise command and control, and utilize various infrastructures. A comprehensive, seamless approach is required to provide the requisite awareness, support, and *response of all participants* throughout the WOG enterprise.

As it is for other warfare domains, it is essential that an integrated approach to an education program, tailored for the various levels of participants from senior leadership through subject matter experts, provide a complete awareness of current procurement requirements and processes, the availability and utilization of intelligence, adversary TTPs, and the fundamental construct of adequate risk assessments and mitigation.

In the near term, we need to better utilize or leverage current authorities of departments, institutions, organizations, and agencies, and re-establish or confirm their roles and responsibilities, with the goal of reducing overall administrative burden,

redundancies, and costs, while vastly improving their effectiveness to combat asymmetric threats.

7. Establish Independently Implemented Automated Assessment and Continuous Monitoring of DIB Software (MT).

Mission-critical systems depend upon complex software assemblies with imperfect assurance. Where DoD programs require the DIB to develop custom software or exploit commercial and open-source software, DoD should require the application of automated validation tools and subject software to independent continuous monitoring for nefarious behavior. Independent validation is especially important where DIB primary and subcontractors use agile or DevOps environments. This may require the creation of a new, independent organization to evaluate the inherent risk within applications and processes, but this is already beginning to happen in the private sector. Ideally, this service should be provided by an independent, unbiased organization such as a not-for-profit or FFRDC. Preliminary conversations indicate that industry is more likely to embrace an assessment or credentialing organization if it is independent of government, though it also must have strong ties to government and the ability to receive and act upon information unique to government sources, including classified information.

Software security is a special risk. Some say, "software is the new hardware" or "software is everything." Software developers rely increasingly upon third-party components for today's complex applications. Much of the software used in devices and systems across all technology types is from multiple sources about which, in all but exceptional cases, little is known. Should adversaries insert malicious functionality into open-source components of software code or exploit latent vulnerabilities, the resulting corruption of the software tool chain can have pervasive and durable effects; these may not result in immediate harm but can be activated at the time chosen by an adversary. Hence, static assessment or static certification by itself is insufficient to ensure protection.

8. Advocate for Litigation Reform and Liability Protection (MT).

For DoD (and the WOG) to achieve and sustain cyber defense and supply chain resilience, government and industry must work together. Government laws and regulations can shape desired industrial behavior. Litigation and potential legal liability also figure prominently as both incentives and constraints on the way industry accomplishes security objectives. This is especially true in the production of software. DoD can lead efforts at litigation reform to manage liability risks and therefore to encourage positive industry behavior and facilitate timely government actions. This subject is addressed in *Annex II.*

9. Ensure Supplier Security and Use Contract Terms (MT).

Industry plays a crucial role. While DoD funds programs, conducts acquisition, and exercises oversight, it relies on the innovation and resources of its industrial base to execute programs and for the technological advantages our warfighters need. Therefore, in dealing with its contractors, DoD should be creating the best environment to ensure supplier security and resilience. Industry is the source of the new technologies to protect those technologies and can provide innovative means, operational and technical, to defend them. Industry often can respond more quickly and with more advanced, difficult-to-defeat technical measures than can government counterparts. Getting the best and most out of industry should be DoD's objective and is a primary element of *Deliver Uncompromised*. Adversaries know to attack those elements of the supply chain that have done the least. For this reason, DoD has to strike a balance—*incentivizing* best practices and company initiative on the one hand but *requiring* sufficient security measures on the other. The ultimate goal of the Department, to reduce *operational risk*, is promoted by measures that supplant *compliance* considerations as drivers and add *positive incentives* for companies to continuously examine and improve their systems and practices. This subject is addressed in *Annex III*.

Elsewhere in this report, we recommend a WOG approach to addressing supply chain resilience and integrated risk management. In some respects, this is only half the equation. As the character of warfare has changed, future battles may be fought, lost, or won within the industrial base. That base includes not only suppliers and integrators that specialize in defense acquisitions, but many other sources—some "commercial" and even "commercial off the shelf (COTS)"—whose products and services are incorporated in defense systems and infrastructure operation. For this reason, next-generation security merits a "whole of industry" approach. Beyond what can be accomplished with companies that are government contractors, leaders should consider how to establish and implement security and resilience standards to cover commercial sources and COTS suppliers. Otherwise, vulnerabilities at the weakest link remain. Because DoD is a major purchaser of supplies and services from the acquisition vehicles of other agencies, such as the General Services Administration Schedule 70 Governmentwide Acquisition Contract or the National Aeronautics and Space Administration Solutions for Enterprise-Wide Procurement, it will be necessary to extend the coverage of contract measures and validation methods to the contracting vehicles of civilian agencies for the acquisition of commercial IT products and product-based services. As demonstrated vividly by the experience with Kaspersky Labs software, attention must extend to commercial software as well as open-source software content that drives systems on which the government and the private sector rely.

10. Extend the 2015 National Defense Authorization Act (NDAA) Section 841 Authorities for "Never Contract with the Enemy" (MT).

The Combatant Commands, being forward-deployed outside the Continental United States, often in hostile and always in high CI threat environments, have unique supply chain and system integrity acquisition (contracting) and operational needs. They lack dedicated DIA/DSS interface, receive little in the way of warning, and when they do, there is no formal requirement for the Commander to act on such potential threats. Formation of the NSIC, as recommended above, would be extremely helpful to the Combatant Commands, as they would ultimately have a handful of liaisons with ready access to threat intelligence. In the meantime, adequate Joint Staff representation with DSS's expanded authorities as elsewhere recommended would support NSIC or interim entities.

To directly address these shortcomings, DPAP has drafted legislation that includes modifications of sections 841-843 of the NDAA, which goes back to 2012 and was modified in 2015. The draft legislation, which was approved by OSD, the Combatant Commands, Office of the General Counsel, and OMB, to shore up operational environment contracting overseas, includes proposed modifications for the 2019 NDAA. DoD should actively engage with Congress and the Executive Branch to build a strong support base to extend these authorities to the Combatant Commands. The recommendations that concern extension of these statutory authorities are summarized in *Annex IV*.

Contractors also have a role to play to avoid purchases from compromised and high-risk sources. Already, leading commercial companies go to great lengths to verify and monitor the trustworthiness of their supply chain. These should become prevailing if not expected practices within the defense supply chain. For certain types of key systems or technologies, it may be necessary to limit suppliers to U.S. sources or to validated international sources. Companies in the DIB should be encouraged to take measures to identify, mitigate, and then eliminate dependencies upon at-risk foreign sources.

11. Institute Innovative Protection of DoD System Design and Operational Information (MT).

Much of U.S. defense and intelligence has confused the concept of "need to know" with "classified." As a result, vast amounts of information regarding system design, trades, vendors, parts lists, operational details, etc., are usually available to *anyone* on the program, and much of it is available to the general public if they desire to go looking for it. Yet the commercial world treats its IP much more carefully and is much stricter concerning not only *who* they share their information with but *how*. Minimally persistent information sharing—much like that used in applications such as

Snapchat—in which minimum information is shared with a subcontractor or vendor via a thin-client network and only available for as long as needed—is becoming industry best practice in some circles. Some elements of the DIB are voluntarily using such techniques on defense contracts without being asked to by the USG. DoD could require such state-of-the-art techniques and compartmentalization based on need-to-know as a part of its basic information protection plan within the Department as well as contractually with suppliers.

Furthermore, where a program is in its life cycle is a determining function of what kind of protective measures are available (see Figure 2). Key capabilities that have been in operational use for decades are likely well known by our adversaries. As a result, their operational assurance risk should be considered high, and for the most vital ones, DoD should seriously consider increasing the ambiguity and uncertainty of the adversary with respect to these programs. Programs early in their life cycle are the easiest to protect, but that commitment needs to be made *at conception* and maintained through the life cycle.

There is a wide range of special options available for the most important programs, but each is different, depending on where the program is in its development cycle (from conception through retirement). The options exercised will become classified, but there will be tens of these, not hundreds.

12. Institute Industry-Standard IT Practices in all Software Developments (MT).

Software Bill of Materials (SBOM)

The software industry has progressed tremendously in the past several decades. Software is the "glue" that binds together components, systems, subsystems, sensors, etc. It is through software instructions that information moves to produce data-based decision making in complex instantiations of hardware. As software has acquired central significance in many systems of ever-expanding complexity, great change has occurred in how software code is created, compiled, and used. The software of complex systems is often built from many discrete software modules that perform distinct functions. Modern software can be rapidly or even automatically assembled. In this respect, software development increasingly resembles manufacturing processes. Thus, it is likely that any given custom or commercially available software system is, in fact, a product of a varied and often complex supply chain. Yet, all too often, and especially with open-source software, little is known concerning the pedigree of the software developer (who owns or controls the developer, for example) or the provenance of the software components (what measures were taken to ensure its integrity and trustworthiness).

In recognition of this fact, good industry practices increasingly mandate the use of an SBOM that identifies the provenance of the various components. If done properly, an SBOM can estimate the overall risk of the ensemble of software elements based on the risk of the individual elements. A dramatic increase in the security of operational software instantiations could be achieved by combining independent continuous monitoring of the development system and operations, independent integrity scoring of the contractor/vendor, and some type of real-time anomaly/event detection for the operational system.

Tracking software composition across the supply chain beyond the primary contractor/vendor is highly recommended and can be leveraged as a contractual term. Acquisition contract language should require the disclosure of commercial, open-source, and third-party software components as part of an SBOM. These disclosures should be independently verified. Knowingly providing false information should be subject to liability for damage and other sanctions against responsible contractors. DoD should not continue to do business with or use software sources that fail to deliver software uncompromised and those that submit false, misleading, or incomplete information. Taking such an approach as this is believed to be consistent with trends in the private sector and is recommended as a tenet of best industry practice.

Secure Software Design Life Cycle (SSDL)

The SSDL is a process DoD could apply to integrate security and integrity into the software development process from concept through decommissioning. This life-cycle approach to the software integrity challenge, blending security and risk identification and management across the acquisition and sustainment boundaries, will require true institutionalization of integrity and accountability in the chain of command. This process should begin with planning and requirements and continue through architecture and design, testing, coding, release, and maintenance. Simply "testing" or "certifying" once during Initial Operating Test and Evaluation is not only inadequate but signals to the adversary exactly when and how to "get past the gate" of security. By utilizing SBOM with continuous monitoring of the development environment coupled with SSDL techniques, this exposure can be reduced, resulting in a tangible realization of software integrity and a greater understanding of risk. The objective is for software security and integrity to become a *continuous* rather than a time-specific concern—from concept to retirement.

DoD can take a wide variety of SSDL approaches to software development that go well beyond the scope of this report. Industry best practices include use of code scanning tools both statically and dynamically and the establishment of realistic security goals and the means to measure progress toward them.

13. Require Vulnerability Monitoring, Coordinating, and Sharing across the Chain of Command for Supply Chain (MT).

While execution of a specific exploit against a particular program or capability may seem local, in reality, it is likely part of a more organized asymmetric offensive strategy against the United States' ability to project force or for the adversary to collect intelligence, steal IP, or otherwise gain a competitive advantage. Therefore, information sharing and the results of vulnerability monitoring are critical elements of an integrated defense. While the NSIC will provide strategic warning and insight into the risks of dealing with individual vendors/contractors or components, valuable information for the counterintelligence picture across the Department comes from the programs and operational Components in the form of self-reporting and observations of anomalous or suspicious activity or behavior. Currently, even within a Service Component, clear examples of incident reporting and potential exploitation are rare. While DSS enjoys a reliable stream of sharing from the DIB, its current purview is constrained to cleared facilities and the contractors using those facilities. Each Service Component in both acquisition and sustainment should look for and coordinate information sharing among themselves and with designated software vulnerability information sharing mechanisms such as the CVE® database, ISAOs, the NTIA, the National Cyber Awareness System of US-CERT, and reports of the Computer Crime and Intellectual Property Section of the DOJ. Many of the COAs recommended by this report reinforce this discovery and sharing.

A vendor vetting database should be created and available to all. This could be championed out of DSS, DPAP, and NSIC. This database would house relevant acquisition, intelligence, and security information related to supply chain risk.

14. Advocate for Tax Incentives and Private Insurance Initiatives (LT).

There is a range of viable options for incentivizing members of the DIB to embrace cyber and supply chain security—especially the smaller subcontractors that are likely to be the most attractive targets of hostile actors. A central theme of this report is that DoD should examine ways to transform risk-management security functions from a cost center to a potential profit center—and a critical differentiator in the source selection process. We have identified and briefly described two categories that would produce positive financial incentives for the DIB—tax and insurance—and suggest other business initiatives to influence private sector actions. These measures would serve the congruent purposes of protecting contractor IP and protecting DoD technical data and other sensitive but unclassified information. DoD can make legislative proposals or otherwise advocate to Congress. This subject is addressed in *Annex V*.

15. For Resilience, Employ Failsafe Mechanisms to Backstop Mission Assurance (LT).

Beyond exploitation aimed at intelligence collection or harvesting of U.S. intellectual property, the objective of asymmetric adversary warfare is to degrade DoD's ability to execute its missions. The adversary has choices among targets. It may be able to achieve its ends largely, even entirely, through asymmetric operations launched against the private sector. An example is where an attack upon commercial logistics systems or transportation infrastructure denies the United States the ability to move forces when and where needed. Adversaries likewise target DoD capabilities directly. As shown in Figure 2, the ultimate exposure of such actions is where the consequence of attack, in the risk equation, produces a "fatal" result—denying readiness for mission. Means must therefore be identified to understand what critical systems are at risk of attack that could reduce them to a non-mission-ready state, and institute techniques that restore systems to a "fixable" state where mission execution continues even in a degraded state until full restoration is achieved.

The high-level, fundamental means of accomplishing resilience, from a system design perspective, is the use of "uncorrelated means of accomplishing the mission." In other words, there should be no single points of failure for critical mission elements—resiliency should be realized through smart system design, implementation, diversity, and redundancy. This can be done at the component, subsystem, system, and even enterprise level. For example, if command and control is singularly dependent upon satellite communications, then alternate means of enabling even degraded communications must be designed into the system to provide a failsafe mechanism. Ideally, different design teams, vendors, and contractors would design these failsafe backups, and collective knowledge of the entire system operation would be closely held. Realistic exercises should be conducted to inform mission owners of where they are at risk and how to recover.

A similar practice is utilized in the commercial world today, although often driven by the extremely high financial cost of loss of operational capability due to non-malicious events. For example, Amazon Web Services has multiple levels of failsafe mechanisms built into its architecture at the board, rack, building, micro geo-location, and macro geo-location—originally to ensure that when someone drops an item in their shopping cart, that information is not lost should a portion of the system fail.

This same type of integrated, integrity-based thinking needs to become pervasive within system engineering and design of DoD capabilities and could be a focus of OSD(R&E).

Conclusion

As a nation, we are at a watershed moment as the character and arguably even the nature of war is changing. There is now overwhelming evidence that adversaries employ blended operations in asymmetric warfare to steal our intellectual property, compromise our technical information, and to degrade, deny, or otherwise damage our factories and critical infrastructure. It is necessary to cast aside historical assumptions that have proven more to trap us than to protect. It is time to put legacy methods behind us. While we should be informed by the past, we should not become its prisoner. Therefore, the Department of Defense must lead initiatives to reduce exposure to hostile acts and enhance security of assets and capabilities. There are many initiatives to be combined and managed. Some affect the internal operations of the Department. Some are directed at the industrial base upon which DoD relies. And some require the coordination of resources among intelligence sources so that threat information can be rapidly processed to produce and appropriately distribute actionable strategic warning. The effort will take time and will present many challenges—but perpetuation of the status quo is unacceptable. We are past the time we can be satisfied with responses that are incidental or merely incremental.

The *Deliver Uncompromised* strategy merits leadership attention and immediate action. In the near term, *Deliver Uncompromised* means that mission owners can trust that the industrial base will not confer technical information or information advantage to adversaries. Means to achieve *Deliver Uncompromised* include elevating *security* as a primary metric for DoD acquisition, forming a Whole of Government National Supply Chain Intelligence Center, using existing acquisition authority and contracting leverage, and taking measures internal to the Department to empower leadership, better inform decision makers, and use accountability to spur results. This all needs to be done in concert with an incentivized and rewarded DIB.

DoD requires a Global Campaign Plan that goes well beyond countering terrorism—one that will defeat asymmetric threats being perpetrated against the United States. This report can serve as the foundation for a comprehensive strategy to defend the procurement and sustainment of the capabilities upon which DoD depends.

Annex I: Contractual Measures

Efforts are needed to create standards for security sufficiency that comprise a "standard of care" expected contractually of every company in the DoD supply chain. Medium and small-sized suppliers frequently complain that they need consistency and coordination in establishing security credentials to the satisfaction of DoD or higher tier contractors. We recommend that DoD and industry establish a system and process to produce SIS, as introduced earlier in this report.

Industry is likely to have more trust in such a system if it is administered by an independent, expert, public-private body that would work with government, standards-setting bodies, industry, academia, technical specialists, and other interested parties. This entity would be able to receive classified materials so that the rating system would reflect the changing threat landscape. We envision the organization acting as an accrediting intermediary. DoD could establish levels or tiers of security sufficiency (Low, Moderate, and High, for example). The public-private entity could work with and for industry to guide, assess, accredit, and even authorize. Credentials received by a supplier through this process could be leveraged to demonstrate assurance to many potential defense customers and other public (or private) sector clients.

This report contains various contracting recommendations. Some will require new regulations and contract clauses. A few might require new statutory authority and rulemaking. To accomplish these will be time-consuming, and there may be uncertainty and questioning from some in the DIB. Those are not reasons to refrain from new action. The plain truth, however unfortunate, is that too many of the Department's present programs and operations already are compro- mised. Expecting better from our adversaries in the future, or believing that these problems will resolve themselves, would cause optimism to triumph over reality. However difficult, bold new action is required, and the acquisition process—broadly understood—is

The "Plain Truth" Calls for Bold Action

The plain truth, however unfortunate, is that too many of the Department's present programs and operations already are compromised. Expecting better from our adversaries in the future, or believing that these problems will resolve themselves, would cause optimism to triumph over reality.

essential to positive change. Below, we summarize key concepts for using contractual leverage:

1. Achievement of minimum security measures can be required for companies (at any level) to participate in the defense supply chain for certain acquisitions.
2. Beyond trusting contractors to provide "adequate security" as required by DFARS 252.204-7012, the Department can establish measures and methods to review and assess actual accomplishment of promised security measures.
3. The Department can work with industry to establish metrics for enterprise-level accreditation of accomplished security using expert third parties for assessment. Use of SIS could motivate improved industry measures.
4. In determining eligibility for new awards, the Department can review the adequacy of required security measures, consider SIS, insist upon specified levels of accreditation, or otherwise

direct requiring activities to make authorization decisions based on their assessment of perceived risk for their specific missions.

5. Where competitive source selection methods are used, DoD can treat security as an evaluation factor and make superior security a positive competitive discriminator. RFPs would inform companies of what is expected and how it will be reviewed.
6. For software assurance, in appropriate contracts DoD can require source code disclosures, minimum maintenance and patching, continuous monitoring, and mandatory event reporting.
7. Using established safeguards, methods, and practices, DoD could establish minimum "standards of due care" such that gross negligence could expose contractors to civil liability or limit their eligibility for future contracts or subcontracts absent satisfactory corrective measures.
8. Contractual "safe harbor" provisions could be used to encourage positive security actions by contractors and to remove present barriers to prompt incident reporting and full cooperation with DoD's assessment and remediation measures.
9. Once appropriate standards are in place, DoD could require contractors to have specified levels of cyber and supply chain insurance.
10. DoD can improve its oversight of contractors to include review of cyber and supply chain assurance measures. DSS can extend its present responsibilities beyond cleared contractors.

Annex II: Litigation Reform Measures

Areas Where Litigation Exposure Should Be Reduced

It is advantageous for DoD that industry reports promptly and fully on known or suspected cyber and supply chain attacks and discovered software vulnerabilities. The DIB and its suppliers need to improve their record of reporting cyber incidents, supply chain vulnerabilities, and assurance failures. Potential litigation risk is part of the problem—both for industry and government.

- Contractors need "safe harbors" to promptly share suspicious or potentially derogatory information with NSIC for its assessment of and appropriate action on potential cyber and supply chain exploitations. Legislation or new regulation may be needed to establish that contractors making good-faith, informed reports on cyber and supply chain attacks will not be exposed to third-party lawsuits challenging the validity of such reports or seeking damages against the reporting entity. For this to occur, contractors need assurance that NSIC can protect the identity of reporting entities and keep reports confidential. NSIC will need to develop protocols on how to disseminate threat and response information based upon the reports.
- DSS has demonstrated the ability to leverage its existing contractual authorities for facility clearances; more robust information sharing on behalf of contractors would go much further with appropriate liability protections. Companies seeking to be treated as "trusted suppliers" can be asked to agree to higher obligations of event reporting and terms of participation in information sharing. New initiatives should be informed by present experience, such as that acquired by the Defense Microelectronics Activity in its trusted accreditation program. In this initiative, DoD must remain cognizant that suppliers will accept costs and burdens of specialized security regimes only if there is a corresponding business case that covers the costs and offers opportunity for profit.

- The government may need litigation reform to act upon industry reports or inputs from other public or non-public sources. Reporting is likely to have the highest value where it can be accomplished quickly. Speed is of the essence. Delays caused by legal review and process can work against the national interest. If the government acts to publish and disseminate contractor-sourced information, it may be exposed to third-party liability under the Federal Tort Claims Act (FTCA), 28 U.S.C. §§ 1346(b), 2671-2680, unless it can claim an exemption such as that for "discretionary function." The exigencies and gravity of cyber and supply chain threats may call for national security exceptions to standing laws and regulations. For example, a new FTCA exception could provide a basis for the federal government to claim immunity from third-party claims arising from cyber alerts and actions.

  DoD and WOG should have a set of tools to benefit its contractors and their suppliers who invest to develop new technologies for cyber and supply chain defense. These can run the gamut of functions—Identify, Protect, Detect, Respond, Recover—that the National Institute of Standards and Technology (NIST) has identified as the Core elements in the *NIST Framework for Improving Critical Infrastructure*.

- The *SAFETY Act*, administered by DHS, encourages investment in anti-terrorism technologies through liability limitations for qualifying, approved products, equipment, service, devices, and technologies. DoD should encourage Congress to extend this aspect of the SAFETY Act to cyber and supply chain security investments. Companies that make such investments and utilize new security systems should face reduced exposure to third-party and government claims following a cyber or supply chain attack. The immunity should extend also to subcontractors and suppliers who employ validated technologies.

- Industry needs to have confidence in the efficacy and expertise of the persons or entities assigned the responsibility to assess and qualify the cyber and supply chain technologies eligible for SAFETY Act liability protection. Consideration is warranted of assigning this function to a trusted third-party intermediary (public or private) that can concentrate expertise, promote new standards and best practices, secure valuable contractor IP, and coordinate with DoD and other government resources for their input and, if appropriate, approval. Potentially, the same independent intermediary that conducts assessments and assigns SIS could perform the SAFETY Act reviews.

Areas Where Liability Risk Might Be Increased

With limited exceptions, it is at best uncertain where or under what circumstances any DoD contractor would face liability to DoD for damages should it fail to fulfill minimum contractual requirements for supply chain and cyber security. Under present law, action could be brought under the False Claims Act for knowing or reckless disregard of cyber obligations, or for intentionally false promises to operate with security that were not fulfilled. To be sure, no contractor or commercial enterprise can guarantee that it will not suffer cyber or supply chain attack, and the fact of attack should never be treated as evidence, itself, of fault on the part of the entity attacked.

Nonetheless, if there is little or no prospect of monetary liability to the DoD customer, and where there may be no financial consequences for bad cyber and supply chain hygiene, some companies may ignore their promises, and others will fail to commit sufficient resources and attention to security improvement. DoD should examine where and on what basis, and with what process, it could expose contractors to contractual damage liability for failure to take reasonable and timely cyber and supply chain assurance measures. Even if the bar is set very high for a contractor to be held liable for breach of expected minimums for assurance, the prospect of such litigation and potential liability may have salutary effects upon

management commitment and company actions. Moreover, the Department may consider whether to seek legislative authority and a regulatory basis to hold its contractors, on selective programs, liable for gross negligence in failure to fulfill cyber and supply chain commitments.

Software liability is an area that merits close attention. Vulnerabilities arise from poor software security, yet it remains the prevailing commercial practice not to make users and operators responsible for software-caused failures and to immunize those who developed the software. For its mission-critical and specially developed software, DoD can demand higher security across the software development life cycle, especially in projects that involve agile or DevOps environments or software refresh during sustainment. Much of the software used in contemporary systems has open-source components with uncertain pedigree or provenance. DoD should consider when to require an SBOM and can encourage Congress to hold hearings on whether to change the law on software immunity—perhaps for certain areas of commerce related to national security and industry and key infrastructure.

It remains true that a hostile actor instigates software, cyber, and supply chain attacks, and therefore, the initiating responsibility resides with the attacker. Today's security environment, however, is one in which such attacks are a fact of life. The attacks are recurring, persistent, diverse, evolving, and highly destructive. In this environment, those who own and operate systems at risk of these threats have a duty of due care to take actions *reasonable*, in light of what they know of threat, vulnerability, and consequence, and *responsible*, considering their resources and technical capabilities. Some analysts have argued that the prospect of civil litigation in the courts and liability for damages will prove important to move the whole of industry to act. The standard of care will figure prominently in what companies do to mitigate litigation risk. DoD has a responsibility to establish and incentivize cyber and supply chain standards that will set a standard of care that is achievable and affordable for the DIB and its suppliers.

Annex III: Ensure Supplier Readiness and Use Contract Terms

The Department should communicate to all levels of the supply chain that integrity is both expected and rewarded, for continuing DoD business, and that *delivering* uncompromised and resilient products is an integral part of contract performance—equal (at least) to cost, schedule, and performance.

Supplier Readiness

DoD can exercise creative options to ensure supplier readiness.

- DoD can work with industry stakeholders to establish cyber and supply chain security standards and practices, and software assurance measures, building off the increasing volume of NIST work that integrates cyber and supply chain measures.

NIST has issued a proposed Revision 5 to SP 800-53 and the Cybersecurity Framework v. 1.1, which encourage important progress in elaboration of combined cyber and supply chain measures. Indeed, the just released SP 800-37 Revision 2 includes the following concise statement of purpose:

"To integrate supply chain risk management (SCRM) concepts into the RMF [Risk Management Framework] to protect against untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the SDLC [System

Development Life Cycle]."
Draft SP 800-37 Rev. 2, at vi.

- As companies act to implement these safeguards, they can be evaluated and assigned into tiers of relative security. Previously in this report, we introduced the idea of SIS. A similar approach is used elsewhere in the federal government. For example, the NIST Cybersecurity Framework articulates four Implementation Tiers in a range from Partial (Tier 1) to Adaptive (Tier 4). Federal Information Processing Standard (FIPS) 199 distinguishes among security impact at levels of Low, Moderate, and High. As elaborated in FIPS 200 and NIST SP 800-53, obligations for controls and enhancements are linked to the impact level of information at risk. The implementation of the Federal Risk and Authorization Management Program (FedRAMP) is particularly instructive. FedRAMP provides a standardized approach to security for cloud computing and for the authorization of cloud services for civilian agencies. In simplified form, FedRAMP produces Authorization to Operate for federal customers for Low-, Moderate-, and High-impact systems. DoD has special requirements for cloud, but again it is a hierarchy of information sensitivity, with more security required for higher Impact Levels. The Defense Information Systems Agency has produced the *Security Requirements Guide,* which adds overlay of both process and substantive security requirements building on FedRAMP, again relying on NIST SP 800-53 as the catalog of available controls.

- For cyber and supply chain assurance, we envision that DoD can work with industry to specify which assurance methods and measures must be met for a contractor to earn a Low, Moderate, or High SIS. Each requiring activity (or each prime contractor) can decide whether its program requires the additional measures (and expense) of a supplier with a higher score, and what evaluation credit to extend for competitors with different score levels. For FedRAMP, the security assessment process is the responsibility of independent third-party assessment organizations working to government-approved process and standards. For the SIS process, we see merit in following a similar approach that allocates the assessment and scoring responsibility to accredited third parties.

- Both suppliers and DoD will benefit if security credentials, established once, can be leveraged across all DoD Requiring Activities. The same approach—"do once, use many times"—can be applied to assessment of suppliers and SIS. Documentation that supports the assigned rating can be available for review by requiring activities within the Department. This prevents duplication of assessment. DoD can require that companies awarded an SIS credential conduct continuous monitoring, and the status as a holder of a credential can be subject to review and renewal at specified intervals. This too is like FedRAMP. It also is similar to the process DSS uses in the grant of Facility Clearance Levels.

It may take some time to establish this credentialing regime, to establish expected methods and assessment process, and to resolve questions of roles and missions among many potentially interested stakeholders. There can be high payoff, however.

Acquisition and Contract Terms

DoD has great influence, through the acquisition process, on the companies that constitute the DIB supply chain. The Department can make better use of these tools to achieve and sustain cyber and supply chain security.

- DoD, through DFARS 252.204-7012, requires all its contractors to have "adequate security" to protect Controlled Unclassified Information (CUI), relying on the 110 safeguards in NIST SP 800-171. Today, there is no method or requirement for assessment, as the implementation is largely trust-based. Moreover, DoD has not assigned a qualified resource to review the actual security accomplishments of

its suppliers. Further, the SP 800-171 safeguards treat all information as having essentially the same, Moderate impact should a breach occur. In addition, DFARS and SP 800-171 focus on the protection of information on or in information systems—with little coverage of supply chain security or operations technology as distinct from IT.

- In the dynamic threat environment, the Department needs to pursue a strategy and campaign to elevate the level and expand the breadth of security achieved, and to implement means of review, assessment, approval or authorization, and oversight. These must be pursued gradually because the present requirements, notwithstanding their limitations, have proven to be very difficult for a sizable percentage of the DIB. DoD must retain the innovation and versatility of the smaller members of the industrial base, and it must work with its prime contractors to assist companies struggling with security requirements. Specifically, DoD should encourage primes and their small business suppliers to shift information systems and applications to qualified, secure cloud service providers. The security outcome for many companies using the cloud will be superior compared to measures taken for on-premises systems. Updates, information management, and cybersecurity are all improved with a cloud provider, since responses can be done on scale and quickly, by not relying on individual patching. DoD is moving aggressively to the cloud, and requiring the DIB and its sub-tired suppliers to follow suit is a logical and practical solution.

- The Department has its greatest leverage, of course, over prime contractors. As evident from Enclosure 14 of Department of Defense Instruction (DoDI) 5000.02, DoD already includes cyber as an objective in the acquisition planning for MDAPs. Similar improvements could be made to DoDI 5000.02, and to the accompanying Defense Acquisition Guidance, to give greater importance to supply chain and software assurance.

- Incorporation of further objectives in acquisition planning should translate to additional definition of cyber, supply chain, and software assurance in program requirements as expressed in Statements of Work and specifications. Funding should accompany these changes, as security has a cost.

- DoD is already acting to inform contractors that they may be required to submit System Security Plans (SSPs) for evaluation and adequacy determination in the source selection process. DoD recently proposed guidance for Contracting Officers on when to request SSPs and how to evaluate their adequacy. Further measures along these lines should be established as security standards and assessment processes develop. DSS, in line with its new emphasis on asset protection, should be considered for increased responsibilities to assess and validate contractor measures to secure CUI.

- Prime contractors undoubtedly will strive to improve and demonstrate their security accomplishments where a source selection includes comparative evaluation and scoring of each offeror's security. At the same time, contractors will insist upon a fair process in which they understand in advance what is expected of them and how it will be evaluated. Having the process defined and resources in place will take some time. But contractors should be informed now that DoD is working to make security a competitive discriminator in future procurements.

- Beyond the prime, as noted, security risks are present at the lower tiers, where DoD has less leverage and no direct contract authority. Clearly, the Department needs to reinforce cyber and supply chain security at every level. Such initiatives will have significant effect upon thousands of private sector enterprises. Some of the responsibility will vest in the primes and higher tier companies. As suggested above, establishing a mechanism for credentialing using common standards and a consistent process will be most helpful. It will

reduce friction within the private sector and avoid unproductive expense and frustration of attempting to conform to multiple, inconsistent reviews and demands.

It may be necessary to reconcile procurement reform with security enhancement. There is widespread enthusiasm for measures to "reform" procurement to reduce barriers to commercial sources, encourage innovation, speed purchase and delivery, and eliminate unproductive regulatory costs. The Department should consider the tension between security objectives and procurement reform. Security measures, as recommended here, should not be just "more cost and time" but should add to the bottom line and be integrated into the procurement process. In acquisition planning, DoD may need to distinguish, and treat separately, acquisitions for high-impact platforms and programs and involving sensitive but unclassified technologies. It will not always be possible both to reform procurement to make it faster, cheaper, and more accessible to commercial suppliers, and to improve and sustain the security of the suppliers. Choices and priorities need to be established and shared with the DIB.

Annex IV: Proposed Section 841-843 NDAA Authority Extensions—Never Contract With the Enemy

	NDAA 2012 Subtitle D—Provisions relating to Contracts in support of Contingency Operations in Iraq & Afghanistan	NDAA 2015 Subtitle E—Never Contract with the Enemy	NDAA 2019 (If enacted into bill) Subtitle X—Never Contract with the Enemy
Applicability	DoD; Contracts greater than $100K performed outside U.S. in CENTCOM AOR	WOG; Contracts performed outside the U.S. greater than $50K, in support of a contingency operation in which members of the Armed Forces are actively engaged in hostilities.	WOG; Contracts performed outside the U.S. (or inside the U.S. to foreign vendor(s)) regardless of dollar value and operation type
Identification Authority	Sec Def through CENTCOM Commander—"identified by the Commander of the United States Central Command"	"the Sec Def shall…establish a program…" (24 Jan 17—OSD formal Legal opinion confirmed Sec Def ID authority until delegated)	Sec Def until delegated down through implementation policy
Identification Criterion	…provides funding directly or indirectly to a person or entity that has been identified by the Commander of the USCENTCOM as actively supporting an insurgency or otherwise actively opposing U.S. or coalition forces in a contingency operation in the USCENTCOM theater of operations. …failed to exercise due diligence to prevent funds from being provided to a person or entity actively opposing U.S. or coalition forces…	(1) provide funds, including goods and services,…directly or indirectly to the enemy (2) fail to exercise due diligence to ensure that none of the funds, including goods and services,…are provided directly or indirectly to the enemy	1) provide funds, including goods and services,…directly or indirectly to a covered person or entity; (2) fail to exercise due diligence to ensure that none of the funds, including goods,… are provided directly or indirectly to a covered person or entity; (3) directly or indirectly support a covered person or entity or otherwise pose a force protection risk to United States Government agencies or Coalition Forces; or (4) pose an unacceptable national security risk.
Covered Person or Entity aka "the Enemy"	Person or entity actively supporting an insurgency or otherwise actively opposing United States or coalition forces in a contingency operation in the United States Central Command theater of operations	A person or entity that is actively opposing United States or coalition forces involved in a contingency operation in which members of the Armed Forces are actively engaged in hostilities.	A person or entity that is (A) engaging in acts of violence against the U.S. Gov't agencies or coalition forces, or providing support, in the form of financing, logistics, training, or intelligence, to those that do; ~~(B) directly or indirectly opposing the interests of U.S. Gov't agencies or coalition forces;~~ (C) engaging in foreign intelligence activities against U.S. Gov't agencies or coalition forces; (D) engaging in transnational organized crime or criminal activities. E) engaging in other activities that present a direct or indirect risk to the national security of the United States or coalition forces;

Annex V: Tax Incentives and Private Insurance Initiatives

Supply Chain Tax Proposals

Tax incentives are a powerful and effective tool to shape corporate behavior in the supply chain process. Tax credits, subsidies, new market incentives, and capital gains rewards are some of the potential ways to make supply chain security investment and deployments profitable. Some proposed recommendations to be explored:

- Tax Credit/Subsidy for Supply Chain Security
  Tax credits or subsidies, such as 26 USC § 48C, or the energy credit in the tax code, have encouraged the use of solar power, wind turbines, fuel cells, and heat pumps. The business energy investment tax credit was passed as part of the Energy Policy Act of 2005 and allows for a 30 percent offset of an investment in an alternative energy system. Similarly, companies that deployed state-of-the-art security would apply for specific tax credits for the taxable year the innovations or products were deployed and could enjoy a similar type of discount. Moreover, tax credits could be used to improve security at lower levels of the supply chain. Apart from encouraging investments by individual vendors and suppliers, a tax credit or rebate could be offered to primes that make investments that improve the means available to subcontractors to improve security, such as offering security as a service.

- New Market Tax Credit Model—Small Businesses
  The new market tax credit program 26 USC § 45D, established as part of the Community Renewals Tax Relief Act of 2000, helped usher in a wave of investment in low-income communities. The credits spurred investments by community development entities and were administered by the Treasury Department. The program was extended by the Tax Relief Unemployment Insurance Reauthorization and Job Creation Act of 2010, and was again reauthorized until 2014. This successful program could be adapted for supply chain purposes. Treasury could extend conditional subsidies as refundable tax credits for security investments by small businesses. If administered by Treasury, thresholds could be established and penalties imposed if fraud or gross negligence were found in a security breach.

- Capital Gains Tax Incentive
  This tax incentive would reward shareholders with a lower capital gains tax on the sale of assets of corporations that had voluntarily adopted certified and well-recognized supply chain security processes, frameworks, and applications. Investors and shareholders would have an economic incentive to pressure boards of directors to adopt state-of-the-art security measures. The approach would produce long-term value creation for shareholders and the corporations. The Securities and Exchange Commission could be a logical enforcement agency that would impose penalties for misrepresentation and help set security metrics.

Supply Chain Insurance Proposals

It has been estimated that the cyber insurance premium market has the potential to reach $7.5 billion in a few years. Currently the market is estimated to be in the $2.5 billion range. At this time there is no standardized federal policy that regulates cyber insurance carriers or coverage. Nothing now requires DIB companies to acquire insurance for cyber or IT processes. Private insurance carriers can play an important role in setting standards for coverage and in the assessment of enterprise security that figures into underwriting decisions. However, insurance coverage today is oriented toward liability protection against the financial consequences of a breach that produces loss of confidentiality of personally identifiable information or other commercial or consumer records subject to privacy requirements. DoD's interests are different. DoD may consider working with the insurance industry and the DIB to establish

coverage objectives, security norms, and use of DFARS contracting tools to require coverage.

It has been noted that the cybersecurity insurance market has remained tentative due to a number of factors—there is a lack of sufficient actuarial data; insurance portfolios do not have standardized categories of risk; and defense contractors lack the information to understand the scope of appropriate coverage. In contrast, the use of risk assessment is well established within the federal government. The recently released *Federal Cybersecurity Risk Determination Report and Action Plan* (May 2018) required by Executive Order 13800 emphasizes risk assessment, as does OMB Memorandum M-17-25 (May 2017). These subjects also are well explored by FIPS-199 and receive new emphasis in the recently released draft of NIST SP 800-37 Rev. 2, which is to "develop the next generation Risk Management Framework (RMF)." These provide a sound foundation for extension of risk assessment methods to the DIB and other private sector enterprises, and will help in establishing a set of agreed-upon metrics and taxonomy for cybersecurity, as they will facilitate increasing and effective use of insurance to improve supply chain security. We propose the following for examination:

- Support Creation of the Cyber Incident Data and Analysis Repository (CIDAR) at DHS or DoD
  The lack of actuarial data has been a major impediment to establishing a robust cyber insurance market and standardized policies. DHS has been exploring the possibility of creating a trusted space so member corporations could share anonymous sensitive cyber incident data, the CIDAR. This data collection and repository would provide this information to appropriate insurers so that standardized policies could be created. The process would help establish standardized categories and a common taxonomy for cyber incidents for the industry. This self-reporting should be conducted under the auspices of the Cybersecurity Information Sharing Act of 2015 (CISA) and its protection from liability (CISA § 106 (b)). The same concept could be undertaken by DoD, independent of DHS, building upon the existing DIB Cybersecurity Program and expanding information sources beyond present members who are cleared contractors and whose participation is voluntary.

- Government as Guarantor—Terrorism Risk Insurance Act (TRIA)
  Government should establish an insurance fund to cover the possibility of a catastrophic supply chain disaster of either a national cross-sector cascading effect of a cyber attack or an attack by a foreign power as an APT. TRIA was passed after 9/11 to provide compensation for large losses resulting from acts of terrorism so insurers would be able to recoup their losses as a national security asset. TRIA ensured the affordability of insurance for terrorism risk, built insurance capacity, and shared the losses between the public and private insurance sectors. In addition, a number of policies in the cyber insurance arena have "acts of war" or "act of God" exclusions, and in the event of a cyber intrusion by a foreign power, both the insured and insurers should have state protection.

- Amend DFARS to Require Insurance Coverage
  A standard contract clause could be added to DFARS requiring contractors to obtain commercial insurance coverage for cyber and supply chain security. The cost of such coverage would be an allowable cost. The Department could work with insurance carriers and industry stakeholders to develop the coverage objectives, metrics, and standards, as well as the methods to be used by carriers to assess and validate the eligibility of contractors for coverage. Accordingly, at the front end, the coverage process would utilize private sector resources (carriers and their third-party assessors) to promote adoption of security measures consistent with DoD's objectives. At the back end, the liability coverage would give assurance to companies that they are protected against direct damages and third-party liability in the event of any breach producing injury to enterprise

operations or compromise of DoD or other source data. This approach also would help establish a baseline of standards and practices and spread cyber and supply chain risk across the marketplace. Just as fire insurance places a number of structural requirements in building codes, based on the requirements of the cyber and supply chain insurance policy, the DIB would have to maintain fundamental standards in a variety of areas, such as (for illustration) encryption of data at rest. New security issues, such as those arising from the increasing use of IoT instrumentalities to connect enterprise systems, also are candidate areas to align DoD objectives with the private insurance industry.

- Use Authority of Public Law 85-804—Indemnification
  This rarely used authority, originally passed during World War II, provides contract relief and indemnification for companies engaged in unusually dangerous activity on behalf of the government. This power could be used to protect private companies against the possibility of extraordinary liability as might arise in working with DoD in high-risk cyber activities, including "full spectrum" measures. Public Law 85-804 also might be applied as a backstop of indemnification to encourage the DIB to share critical information on cyber breaches, should the existing CISA mechanism prove inadequate.

Other Supply Chain Measures

- IP Trusts and "Golden Shares"
  DoD remains reliant upon global sources, but some technologies and some sources are more critical than others. Measures may be needed to protect against the loss of specific sources or technology. The Department could enter into agreements with some DIB participants to create IP Trusts between prime contractors and key suppliers. The primes would be trustees, with the DoD as the third-party beneficiary. The trusts would protect the critical IP and companies entering the trust. In certain specified events, such as a change of control presenting concerns of foreign ownership, control, or influence, or where there is a disabling security breach at the subcontractor level, DoD could exercise its authority as trustee to recover IP in an uncompromised state. In the area of software assurance, a trust mechanism might be used to assure DoD that it has the gold standard of code for purposes of forensics, patch management, or other security or restorative measures. DoD could also be granted "golden shares" in the trust that would allow it to outvote all board members. In the event of a critical bankruptcy or potential sale, the authority over the golden shares would allow DoD to shape the outcome, enabling it to condition approval upon adequate mitigation measures or, if necessary, block ownership or technology transfers altogether, where potential transactions are found to violate national security interests.

Biographies

Christopher Nissen
Director, Asymmetric Threat
Response Special Concepts Group
The MITRE Corporation

Christopher Nissen is Director of Asymmetric Threat Response at The MITRE Corporation, a not-for-profit which operates and manages seven FFRDCs serving in the national interest. He works across the corporation developing essential strategic elements to address non-kinetic, full-spectrum asymmetric threats to national security in both the public and private sectors. He has developed extensive work programs in these and other domains across the technology, policy, and legislative solution spaces. He has also served as Director of the Communications and Networking Technical Center, leading a division of over 230 engineers in a diverse portfolio of programs and technology development spanning microelectronics to satellite communications.

He has 30 years of experience in developing solutions for extremely complex national security challenges. Some of his accomplishments include putting forth an original vision for the development of an anti-jam capability for the nation's Global Positioning Satellite system, and the development and implementation of several special communications techniques. He holds BSEE and MSEE degrees and also has a background in structured analytical techniques.

John E. Gronager, Ph.D.
Director, Special Enterprise Capabilities

Dr. Gronager recently joined The MITRE Corporation as the Director of Special Enterprise Capabilities within the MITRE National Security Sector. He serves as a senior technical contributor in MITRE's cyber, critical infrastructure, nuclear, and supply chain work programs. In collaboration with MITRE's work program leaders, Dr. Gronager has worked to develop MITRE's work program, create intellectual capital, and identify and develop talent in these critical areas.

Before joining MITRE, Dr. Gronager had 38 years' experience in managing technical programs across the national security mission of Sandia National Laboratories. As a former Distinguished Member of the Technical Staff and Senior Manager, Dr. Gronager developed and managed programs in nuclear reactor safety, nuclear weapons design, testing, and manufacturing, the national transportation infrastructure, international security programs, and for over 28 years provided support to the Intelligence Community.

Robert S. Metzger, J.D.
Shareholder, ROGERS JOSEPH O'DONNELL,
a Professional Law Corporation

Robert S. Metzger, an attorney in private practice, heads the Washington, DC, office of Rogers Joseph O'Donnell, P.C., a firm that has specialized in public contract matters for more than 35 years. He has an active practice that includes civil and administrative litigation, compliance counseling, national security matters, export issues, and other regulatory advice. Mr. Metzger represents leading U.S. and international technology companies in several industry sectors.

Mr. Metzger is recognized for subject area leadership in cyber, supply chain, and related security subjects and has many publications on these subjects. Named a 2016 "Federal 100" awardee, he was cited by *Federal Computer Week* for his "ability to integrate policy, regulation and technology." *Federal Computer Week* said of him, "In 2015, he was at the forefront of the convergence of the supply chain and cybersecurity, and his work continues to influence the strategies of federal entities and companies alike."

Chambers USA (2018) ranks him among top government contracts lawyers and said that "[h]e is particularly noted for his expertise in cyber and supply-chain security with clients regarding him as the 'preeminent expert in cybersecurity regulations and how they affect government contractors.'"

For RSA Conference 2018, Mr. Metzger served on a panel on "First Recourse or Last Resort? The National Interest in Regulating the IoT" and moderated a second panel on "IOT and Critical Infrastructures: A Collision of Fundamentals?" For RSA Conference 2017, he moderated a discussion on "Cyber/physical Security and the IoT: National Security Considerations." A member of the International Institute for Strategic Studies, his articles on national security topics have appeared in *International Security* and the *Journal of Strategic Studies*, among other publications.

The Legal 500 in 2016 cites Mr. Metzger as an "expert" in cyber and supply chain security; in prior years, he was recognized by *The Legal 500* for telecommunications (litigation and appellate). He is among the 49 U.S. lawyers rated as "Expert" in government contracts by *Who's Who Legal* (2016, 2017). He was featured in the Government Contracts 2017 Discussion of *Who's Who Legal*.

Mr. Metzger attended Georgetown University Law Center, where he was an Editor of the *Georgetown Law Journal*. Subsequently, he was a Research Fellow, Center for Science & International Affairs, Harvard Kennedy School (now, "Belfer Center"). As a Special Government Employee of the Department of Defense, he was a member of the Defense Science Board task force that produced the Cyber Supply Chain Report in April 2017.

Mr Metzger served as a subject-matter expert subcontractor to The MITRE Corporation for this study.

Harvey Rishikof, J.D.

Harvey Rishikof's career includes experiences in the private sector, academia, and public service. He is a lifetime member of the Council on Foreign Relations and the American Law Institute. Mr. Rishikof is currently Senior Advisor to the American Bar Association (ABA) Cybersecurity Legal Task Force, Chair of the Advisory Committee to the ABA Standing Committee on Law and National Security, and is working on a number of projects with MITRE and the MacArthur Foundation. For the next year he will be a Visiting Professor at Temple Law School. Mr. Rishikof was a Teaching Professor and Director of the Cybersecurity and the Law program in the iSchool and Earle Mack School of Law at Drexel University. He is the former Convening Authority for the Military Commissions and senior policy advisor to the director of the National Counterintelligence Executive in the Office of the Director of National Intelligence. He has held several positions in the National War College (NWC) at the National Defense University in Washington, DC, including Dean of the NWC, Chair of the Department of National Security Strategy, and Professor of Law and National Security Studies. Academically and professionally, Mr. Rishikof specializes in the areas of national security, civil and military courts, terrorism, international law, civil liberties, and the U.S. Constitution.

He is a former member of the law firm Hale and Dorr, the former Dean of the Roger Williams University School of Law, in Bristol, RI, and has been a consultant to the World Bank and the USAID on law reform. As Legal Counsel to the Deputy Director of the FBI, he focused on FBI policies concerning national security and terrorism, and served as liaison to the Office of the Attorney General at the Department of Justice. He worked on developing a variety of programs (e.g., the National Integrated Ballistic Information Network), and was involved in the drafting of Presidential Decision Directives in the national security area.

As Administrative Assistant to the Chief Justice of the Supreme Court (1994-96), Mr. Rishikof, a former federal court of appeals law clerk in the Third Circuit for the Honorable Leonard I. Garth, served as chief of staff for the Chief Justice and was involved in general policy issues concerning the federal court system. In this capacity, he acted as liaison to the Executive Branch, Congress, the Federal Judicial Center, and the Administrative Office of the United States Court.

Mr. Rishikof has participated in numerous international seminars and projects in Latin America, Europe, Russia, Southeast Asia, Pakistan, India, and China. His most recent books are co-edited with Roger George, *The National Security Enterprise–Navigating the Labyrinth* (Georgetown Press, 2d ed. Quad 2017) and co-edited with Stewart Baker and Bernard Horowitz, *Patriots Debate–Contemporary Issues in National Security Law* (ABA Press, 2012). Mr. Rishikof has participated in numerous international seminars and projects in Latin America, Europe, Russia, SE Asia, Pakistan, India, and China. His publications include *Morality, Ethics, and Law in the War on Terrorism (The Long War)*, part of

the West Point terrorism series Countering Terrorism and Insurgency in the 21st Century: International Perspectives.

Mr. Rishikof holds a JD from New York University School of Law, an MA from Brandeis University, an MA from the National War College, and a BA from McGill University.

Mr. Rishikof served as a subject-matter expert subcontractor to The MITRE Corporation for this study.

Acronyms

A&S	Acquisition and Sustainment
ABA	American Bar Association
APT	Advanced Persistent Threat
CI	Counterintelligence
CIDAR	Cyber Incident Data and Analysis Repository
CISA	Cybersecurity Information Sharing Act of 2015
COA	Course of Action
COTS	Commercial off the Shelf
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DEPSEC-DEF	Deputy Secretary of Defense
DHS	Department of Homeland Security
DIA	Defense Information Agency
DIB	Defense Industrial Base
DNI	Director of National Intelligence
DoD	Department of Defense
DODI	Department of Defense Instruction
DOJ	Department of Justice
DPAP	Defense Procurement and Acquisition Policy
DSS	Defense Security Service
DU	Deliver Uncompromised
FBI	Federal Bureau of Investigation
FedRAMP	Federal Risk and Authorization Management Program
FFRDC	FederallyFundedResearchandDevelopmentCenter
FIPS	Federal Information Processing Standard
FPAP	Field-Programmable Gate Array
FTCA	Federal Tort Claims Act
IC	Intelligence Community
IoT	Internet of Things
IP	Intellectual Property

ISAO	Information Sharing and Analysis Organization
IT	Information Technology
LT	Long Term
MDAP	Major Defense Acquisition Program
MT	Medium Term
NCSC	NationalCounterintelligenceandSecurityCenter
NCSC	National Counterintelligence Security Center
NCTC	National Counterterrorism Center
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NSIC	National Supply Chain Intelligence Center
NTIA	National Telecommunications and Information Administration
NWS	National War College
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
OTA	Other Transaction Agreement
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
R&E	Research and Engineering
RFP	Request for Proposal
SBOM	Software Bill of Materials
SCRM-TAC	SupplyChainRiskManagement–ThreatAnalysis Cell
SIS	Security Integrity Score
SSDL	Software Design Life Cycle
SSP	System Security Plan
ST	Short Term
TRIA	Terrorism Risk Insurance Act
TSN	Trusted Systems and Networks
TTPs	Tactics, Techniques, and Procedures
US-CERT	UnitedStatesComputerEmergencyReadinessTeam
USD(I)	Under Secretary of Defense for Intelligence
USG	U.S. Government
WOG	Whole-of-Government

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.
As prescribed in 204.7304(c), use the following clause:

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)

(a) *Definitions*. As used in this clause—

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

"Forensic analysis" means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Malicious software" means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

"Media" means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

"Operationally critical support" means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

"Rapidly report" means within 72 hours of discovery of any cyber incident.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation

and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) *Cyber incident reporting requirement.*

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

(3) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber

incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

(d) *Malicious software*. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis*. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DoD safeguarding and use of contractor attributional/proprietary information*. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD*. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DoD*. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements*. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts*. The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204, 212, 217, and 252

[Docket DARS–2020–0034]

RIN 0750–AJ81

Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Interim rule.

SUMMARY: DoD is issuing an interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain.

DATES: Effective November 30, 2020.

Comments on the interim rule should be submitted in writing to the address shown below on or before November 30, 2020, to be considered in the formation of a final rule.

ADDRESSES: Submit comments identified by DFARS Case 2019–D041, using any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Search for "DFARS Case 2019–D041". Select "Comment Now" and follow the instructions provided to submit a comment. Please include "DFARS Case 2019–D041" on any attached documents.
- *Email: osd.dfars@mail.mil.* Include DFARS Case 2019–D041 in the subject line of the message.

Comments received generally will be posted without change to *http://www.regulations.gov,* including any personal information provided. To confirm receipt of your comment(s), please check *www.regulations.gov,* approximately two to three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: Ms. Heather Kitchens, telephone 571–372–6104.

SUPPLEMENTARY INFORMATION:

I. Background

The theft of intellectual property and sensitive information from all U.S. industrial sectors due to malicious cyber activity threatens economic security and national security. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Over a ten-year period, that burden would equate to an estimated $570 billion to $1.09 trillion dollars in costs. As part of multiple lines of effort focused on the security and resiliency of the Defense Industrial Base (DIB) sector, the Department is working with industry to enhance the protection of unclassified information within the supply chain. Toward this end, DoD has developed the following assessment methodology and framework to assess contractor implementation of cybersecurity requirements, both of which are being implemented by this rule: the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 DoD Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC) Framework. The NIST SP 800–171 DoD Assessment and CMMC assessments will not duplicate efforts from each assessment, or any other DoD assessment, except for rare circumstances when a re-assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance.

A. NIST SP 800–171 DoD Assessment Methodology

DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is included in all solicitations and contracts, including those using Federal Acquisition Regulation (FAR) part 12 commercial item procedures, except for acquisitions solely for commercially available off-the-shelf (COTS) items. The clause requires contractors to apply the security requirements of NIST SP 800–171 to "covered contractor information systems," as defined in the clause, that are not part of an IT service or system operated on behalf of the Government. The NIST SP 800–171 DoD Assessment Methodology provides for the assessment of a contractor's implementation of NIST SP 800-171 security requirements, as required by DFARS clause 252.204–7012. More information on the NIST SP 800–171 DoD Assessment Methodology is available at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

The Assessment uses a standard scoring methodology, which reflects the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor, and three assessment levels (Basic, Medium, and High), which reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment. A Basic Assessment is a self-assessment completed by the contractor, while Medium or High Assessments are completed by the Government. The Assessments are completed for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order.

The results of Assessments are documented in the Supplier Performance Risk System (SPRS) at *https://www.sprs.csd.disa.mil/* to provide DoD Components with visibility into the scores of Assessments already completed; and verify that an offeror has a current (*i.e.,* not more than three years old, unless a lesser time is specified in the solicitation) Assessment, at any level, on record prior to contract award.

B. Cybersecurity Maturity Model Certification Framework

Building upon the NIST SP 800–171 DoD Assessment Methodology, the CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB contractor can adequately protect sensitive unclassified information such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

The CMMC model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community. The CMMC levels and the associated sets of processes and practices are cumulative. The CMMC model encompasses the basic safeguarding requirements for FCI specified in FAR clause 52.204–21, Basic Safeguarding of Covered

Contractor Information Systems, and the security requirements for CUI specified in NIST SP 800–171 per DFARS clause 252.204–7012. Furthermore, the CMMC model includes an additional five processes and 61 practices across Levels 2–5 that demonstrate a progression of cybersecurity maturity.

Level	Description
1	Consists of the 15 basic safeguarding requirements from FAR clause 52.204–21.
2	Consists of 65 security requirements from NIST SP 800–171 implemented via DFARS clause 252.204–7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3.
3	Consists of all 110 security requirements from NIST SP 800–171, 20 CMMC practices, and 3 CMMC processes.
4	Consists of all 110 security requirements from NIST SP 800–171, 46 CMMC practices, and 4 CMMC processes.
5	Consists of all 110 security requirements from NIST SP 800–171, 61 CMMC practices, and 5 CMMC processes.

In order to achieve a specific CMMC level, a DIB company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level. CMMC assessments will be conducted by accredited CMMC Third Party Assessment Organizations (C3PAOs). Upon completion of a CMMC assessment, a company is awarded a certification by an independent CMMC Accreditation Body (AB) at the appropriate CMMC level (as described in the CMMC model). The certification level is documented in SPRS to enable the verification of an offeror's certification level and currency (*i.e.* not more than three years old) prior to contract award. Additional information on CMMC and a copy of the CMMC model can be found at *https://www.acq.osd.mil/cmmc/index.html.*

DoD is implementing a phased rollout of CMMC. Until September 30, 2025, the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, is prescribed for use in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, excluding acquisitions exclusively for COTS items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement the phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment.

CMMC will apply to all DoD solicitations and contracts, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, starting on or after October 1, 2025. Contracting officers will not make award, or exercise an option on a contract, if the offeror or contractor does not have current (*i.e.* not older than three years) certification for the required CMMC level. Furthermore, CMMC certification requirements are required to be flowed down to subcontractors at all tiers, based on the sensitivity of the unclassified information flowed down to each subcontractor.

II. Discussion and Analysis

A. NIST SP 800–171 DoD Assessment Methodology

This rule amends DFARS subpart 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting, to implement the NIST SP 800–171 DoD Assessment Methodology. The new coverage in the subpart directs contracting officers to verify in SPRS that an offeror has a current NIST SP 800–171 DoD Assessment on record, prior to contract award, if the offeror is required to implement NIST SP 800–171 pursuant to DFARS clause 252.204–7012. The contracting officer is also directed to include a new DFARS provision 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements, and a new DFARS clause 252.204–7020, NIST SP 800–171 DoD Assessment Requirements, in solicitations and contracts including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of COTS items.

The new DFARS provision 252.204–7019 advises offerors required to implement the NIST SP 800–171 standards of the requirement to have a current (not older than three years) NIST SP 800–171 DoD Assessment on record in order to be considered for award. The provision requires offerors to ensure the results of any applicable current Assessments are posted in SPRS and provides offerors with additional information on conducting and submitting an Assessment when a current one is not posted in SPRS.

The new DFARS clause 252.204–7020 requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level Assessment. The clause also requires the contractor to ensure that applicable subcontractors also have the results of a current Assessment posted in SPRS prior to awarding a subcontract or other contractual instruments. The clause also provides additional information on how a subcontractor can conduct and submit an Assessment when one is not posted in SPRS, and requires the contractor to include the requirements of the clause in all applicable subcontracts or other contractual instruments.

B. Cybersecurity Maturity Model Certification

This rule adds a new DFARS subpart, Subpart 204.75, Cybersecurity Maturity Model Certification (CMMC), to specify the policy and procedures for awarding a contract, or exercising an option on a contract, that includes the requirement for a CMMC certification. Specifically, this subpart directs contracting officers to verify in SPRS that the apparently successful offeror's or contractor's CMMC certification is current and meets the required level prior to making the award.

A new DFARS clause 252.204–7021, Cybersecurity Maturity Model Certification Requirements, is prescribed for use in all solicitations and contracts or task orders or delivery orders, excluding those exclusively for the acquisition of COTS items. This DFARS clause requires a contractor to: Maintain the requisite CMMC level for the duration of the contract; ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments; and include the requirements of the clause in all subcontracts or other contractual instruments.

The Department took into consideration the timing of the requirement to achieve a CMMC level certification in the development of this rule, weighing the benefits and risks associated with requiring CMMC level certification: (1) At time of proposal or offer submission; (2) at time of award;

or (3) after contract award. The Department ultimately adopted alternative 2 to require certification at the time of award. The drawback of alternative 1 (at time of proposal or offer submission) is the increased risk for contractors since they may not have sufficient time to achieve the required CMMC certification after the release of the Request for Information (RFI). The drawback of alternative 3 (after contract award) is the increased risk to the Department with respect to the schedule and uncertainty with respect to the case where the contractor is unable to achieve the required CMMC level in a reasonable amount of time given their current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI. The Department seeks public comment on the timing of contract award, to include the effect of requiring certification at time of award on small businesses.

C. Conforming Changes

This rule also amends the following DFARS sections to make conforming changes:

- Amends the list in DFARS section 212.301 of solicitation provisions and contract clauses that are applicable for the acquisition of commercial items to include the provisions and clauses included in this rule.
- Amends DFARS 217.207, Exercise of Options, to advise contracting officers that an option may only be exercised after verifying the contractor's CMMC level, when CMMC is required in the contract.

III. Applicability to Contracts at or Below the Simplified Acquisition Threshold and for Commercial Items, Including Commercially Available Off-the-Shelf Items

This rule creates the following new solicitation provision and contract clauses:

- DFARS 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements;
- DFARS clause 252.204–7020, NIST SP 800–171 DoD Assessment Requirements; and
- DFARS clause 252.204–7021, Cybersecurity Maturity Model Certification Requirements.

The objective of this rule is provide the Department with: (1) The ability to assess contractor implementation of NIST SP 800–171 security requirements, as required by DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting; and (2) assurances that DIB contractors can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information flowed down to subcontractors in a multi-tier supply chain. Flowdown of the requirements is necessary to respond to threats that reach even the lowest tiers in the supply chain. Therefore, to achieve the desired policy outcome, DoD intends to apply the new provision and clauses to contracts and subcontracts for the acquisition of commercial items and to acquisitions valued at or below the simplified acquisition threshold, but greater than the micro-purchase threshold. The provision and clauses will not be applicable to contracts or subcontracts exclusively for the acquisition of commercially available off-the-shelf items.

IV. Expected Cost Impact and Benefits

A. Benefits

The theft of intellectual property and sensitive information from all U.S. industrial sectors due to malicious cyber activity threatens U.S. economic and national security. The aggregate loss of intellectual property and certain unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation, as well as significantly increase risk to national security. This rule is expected to enhance the protection of FCI and CUI within the DIB sector.

B. Costs

A Regulatory Impact Analysis (RIA) that includes a detailed discussion and explanation about the assumptions and methodology used to estimate the cost of this regulatory action is available at *www.regulations.gov* (search for "DFARS Case 2019–D041" click "Open Docket," and view "Supporting Documents"). The total estimated public and Government costs (in millions) associated with this rule, calculated in perpetuity in 2016 dollars at a 7 percent discount rate, is provided as follows:

Total cost (in millions)	Public	Govt	Total
Annualized Costs	$6,500.5	$0.3	$6,500.7
Present Value Costs	92,863.6	3.7	92,867.3

The following is a breakdown of the public and Government costs and savings associated with each component of the rule:

1. NIST SP 800–171 DoD Assessments

The following is a summary of the estimated public and Government costs (in millions) associated with the NIST SP DoD Assessments, calculated in perpetuity in 2016 dollars at a 7 percent discount rate:

DoD assessments	Public	Government	Total
Annualized Costs	$6.7	$9.5	$16.3
Present Value Costs	96.1	136.2	232.3

2. CMMC Requirements

The following is a summary of the estimated public and Government costs (in millions) associated with the CMMC requirements, calculated in perpetuity in 2016 dollars at a 7 percent discount rate:

CMMC requirements	Public	Government	Total
Annualized Costs	$6,525.0	$8.9	$6,533.9
Present Value Costs	93,213.6	127.3	93,340.9

3. Elimination of Duplicate Assessments

The following is a summary of the estimated public and Government savings (in millions) associated with the elimination of duplicate assessments, calculated in perpetuity in 2016 dollars at a 7 percent discount rate:

Eliminate duplication	Public	Government	Total
Annualized Savings	-$31.2	-$18.2	-$49.4
Present Value Savings	-446.1	-259.8	-705.9

V. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is an economically significant regulatory action and, therefore, was subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is a major rule under 5 U.S.C. 804.

VI. Executive Order 13771

The rule is not subject to the requirements if E.O. 13771, because this rule is being issued with respect to a national security function of the United States.

VII. Regulatory Flexibility Act

DoD expects this rule to have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.* Therefore, an initial regulatory flexibility analysis has been performed and is summarized as follows:

A. Reasons for the Action

This rule is necessary to address threats to the U.S. economy and national security from ongoing malicious cyber activities, which includes the theft of hundreds of billions of dollars of U.S. intellectual property. Currently, the FAR and DFARS prescribe contract clauses intended to protect FCI and CUI within the DoD supply chain. Specifically, the clause at FAR 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, is prescribed at FAR 4.1903 for use in Government solicitations and contracts and requires contractors and subcontractors to apply basic safeguarding requirements when processing, storing, or transmitting FCI in or from covered contractor information systems. The clause focuses on ensuring a basic level of cybersecurity hygiene and is reflective of actions that a prudent business person would employ.

In addition, DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires defense contractors and subcontractors to provide "adequate security" to store, process, or transmit CUI on information systems or networks, and to report cyber incidents that affect these systems or networks. The clause states that to provide adequate security, the Contractor shall implement, at a minimum, the security requirements in "National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations." Contractors are also required to flow down DFARS Clause 252.204–7012 to all subcontracts, which involve CUI.

However, neither the FAR clause, nor the DFARS clause, provide for DoD verification of a contractor's implementation of basic safeguarding requirements or the security requirements specified in NIST SP 800–171 prior to contract award.

Under DFARS clause 252.204–7012, DIB companies self-attest that they will implement the requirements in NIST SP 800–171 upon submission of their offer. A contractor can document implementation of the security requirements in NIST SP 800–171 by having a system security plan in place to describe how the security requirements are implemented, in addition to associated plans of action to describe how and when any unimplemented security requirements will be met. As a result, the current regulation enables contractors and subcontractors to process, store, or transmit CUI without having implemented all of the 110 security requirements and without establishing enforceable timelines for addressing shortfalls and gaps.

Findings from DoD Inspector General report (DODIG–2019–105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information. The report emphasizes that malicious actors can exploit the vulnerabilities of contractors' networks and systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies.

Although DoD contractors must include DFARS clause 252.204–7012 in subcontracts for which subcontract performance will involve covered defense information (DoD CUI), this does not provide the Department with sufficient insights with respect to the cybersecurity posture of DIB companies throughout the multi-tier supply chain for any given program or technology development effort.

Furthermore, given the size and scale of the DIB sector, the Department cannot scale its organic cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors every three years. As a result, the Department's organic assessment capability is best suited for conducting targeted assessments for a subset of DoD contractors.

Finally, the current security requirements specified in NIST SP 800–171 per DFARS clause 252.204–7012, do not sufficiently address additional threats to include Advanced Persistent Threats (APTs).

Because of these issues and shortcomings and the associated risks to national security, the Department determined that the status quo was not acceptable and developed a two-pronged approach to assess and verify the DIB's ability to protect the FCI and CUI on its information systems or networks, which is being implemented by this rule:

- *The National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 DoD Assessment Methodology.* A standard methodology to assess contractor implementation of the cybersecurity requirements in NIST SP 800–171,

"Protecting Controlled Unclassified Information (CUI) In Nonfederal Systems and Organizations."

• *The Cybersecurity Maturity Model Certification (CMMC) Framework.* A DoD certification process that measures a company's institutionalization of processes and implementation of cybersecurity practices.

B. Objectives of, and Legal Basis for, the Rule

This rule establishes a requirement for contractors to have a current NIST SP 800–171 DoD Assessment and the appropriate CMMC level certification prior to contract award and during contract performance. The objective of the rule is to provide the Department with: (1) The ability to assess at a corporate-level a contractor's implementation of NIST SP 800–171 security requirements, as required by DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting; and (2) assurances that a DIB contractor can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

1. NIST SP 800–171 DoD Assessment Methodology

In February 2019, the Under Secretary of Defense for Acquisition and Sustainment directed the Defense Contract Management Agency (DCMA) to develop a standard methodology to assess contractor implementation of the cybersecurity requirements in NIST SP 800–171 at the corporate or entity level. The DCMA Defense Industrial Base Cybersecurity Assessment Center's NIST SP 800–171 DoD Assessment Methodology is the Department's initial strategic DoD/corporate-wide assessment of contractor implementation of the mandatory cybersecurity requirements established in the contracting regulations. Results of a NIST SP 800–171 DoD Assessment reflect the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor, and may be conducted at one of three assessment levels. The DoD Assessment Methodology provides the following benefits:

• *Enables Strategic Assessments at the Entity-level.* The NIST SP 800–171 DoD Assessment Methodology enables DoD to strategically assess a contractor's implementation of NIST SP 800–171 on existing contracts that include DFARS clause 252.204–7012, and to provide an objective assessment of a contractor's NIST SP 800–171 implementation status.

• *Reduces Duplicative or Repetitive Assessments of our Industry Partners.* Assessment results will be posted in the Supplier Performance Risk System (SPRS), DoD's authoritative source for supplier and product performance information. This will provide DoD Components with visibility to summary level scores, rather than addressing implementation of NIST SP 800–171 on a contract-by-contract approach. Conducting such assessments at a corporate- or entity-level, significantly reduces the need to conduct assessments at the program or contract level, thereby reducing the cost to both DoD and industry.

• *Provides a Standard Methodology for Contractors to Self-assess Their Implementation of NIST SP 800–171.* The Basic Assessment provides a consistent means for contractors to review their system security plans prior to and in preparation for either a DoD or CMMC assessment.

The NIST SP 800–171 DoD Assessment Methodology provides a means for the Department to assess contractor implementation of these requirements as the Department transitions to full implementation of the CMMC, and a means for companies to self-assess their implementation of the NIST SP 800–171 requirements prior to either a DoD or CMMC assessment.

2. The CMMC Framework

Section 1648 of the National Defense Authorization Act for Fiscal Year (FY) 2020 (Pub. L. 116–92) directs the Secretary of Defense to develop a risk-based cybersecurity framework for the DIB sector, such as CMMC, as the basis for a mandatory DoD standard. Building upon the NIST SP 800–171 DoD Assessment Methodology, the CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB contractor can adequately protect sensitive unclassified information (*i.e.* FCI and CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. Implementation of the CMMC Framework is intended to solve the following policy problems:

• *Verification of a contractor's cybersecurity posture.* DFARS clause 252.204–7012 does not provide for the DoD verification of a DIB contractor's implementation of the security requirements specified in NIST SP 800–171 prior to contract award. DIB companies self-attest that they will implement the requirements in NIST SP 800–171 upon submission of their offer. Findings from DoD Inspector General report (DODIG–2019–105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information. CMMC adds the element of verification of a DIB contractor's cybersecurity posture through the use of accredited C3PAOs. The company must achieve the CMMC level certification required as a condition of contract award.

• *Comprehensive implementation of cybersecurity requirements.* Under DFARS clause 252.204–7012, a contractor can document implementation of the security requirements in NIST SP 800–171 by having a system security plan in place to describe how the security requirements are implemented, in addition to associated plans of action to describe how and when any unimplemented security requirements will be met. The CMMC framework does not allow a DoD contractor or subcontractor to achieve compliance status through the use of plans of action. In general, CMMC takes a risk-based approach to addressing cyber threats. Based on the type and sensitivity of the information to be protected, a DIB company must achieve the appropriate CMMC level and demonstrate implementation of the requisite set of processes and practices. Although the security requirements in NIST SP 800–171 addresses a range of threats, additional requirements are needed to further reduce the risk of Advanced Persistent Threats (APTs). An APT is an adversary that possesses sophisticated levels of expertise and significant resources, which allow it to create opportunities to achieve its objectives by using multiple attack vectors (*e.g.* cyber, physical, and deception). The CMMC model includes additional processes and practices in Levels 4 and 5 that are focused on further reducing the risk of APT threats. The CMMC implementation will provide the Department with an ability to illuminate the supply chain, for the first time, at scale across the entire DIB sector. The CMMC framework requires contractors to flow down the appropriate CMMC

certification requirement to subcontractors throughout the entire supply chain. DIB companies that do not process, store, or transmit CUI, must obtain a CMMC level 1 certification. DIB companies that process, store, or transmit CUI must achieve a CMMC level 3 or higher, depending on the sensitivity of the information associated with a program or technology being developed.

- *Scale and Depth.* DoD contractors must include DFARS clause 252.204–7012 in subcontracts for which subcontract performance will involve covered defense information (DoD CUI), but this does not provide the Department with sufficient insights with respect to the cybersecurity posture of DIB companies throughout the multi-tier supply chain for any given program or technology development effort. Given the size and scale of the DIB sector, the Department cannot scale its organic cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors every three years. As a result, the Department's organic assessment capability is best suited for conducting targeted assessments for a subset of DoD contractors that support prioritized programs and/or technology development efforts. CMMC addresses the challenges of the Department scaling its organic assessment capability by partnering with an independent, non-profit CMMC–AB that will accredit and oversee multiple third party assessment organizations (C3PAOs) which in turn, will conduct on-site assessments of DoD contractors throughout the multi-tier supply chain. DIB companies will be able to directly schedule assessments with an accredited C3PAO for a specific CMMC level. The cost of these CMMC assessments will be driven by multiple factors including market forces, the size and complexity of the network or enclaves under assessment, and the CMMC level.
- *Reduces Duplicate or Repetitive Assessments of our Industry Partners.* Assessment results will be posted in the Supplier Performance Risk System (SPRS), DoD's authoritative source for supplier and product performance information. This will provide DoD Components with visibility to CMMC certifications for DIB contractor networks and an alternative to addressing implementation of NIST SP 800–171 on a contract-by-contract approach—significantly reducing the need to conduct assessments at the program level, thereby reducing the cost to both DoD and industry.

C. Description of and Estimate of the Number of Small Entities to Which the Rule Will Apply

This rule will impact all small businesses that do business with Department of Defense, except those competing on contracts or orders that are exclusively for COTS items or receiving contracts or orders valued at or below the micro-purchase threshold.

1. The NIST SP 800–171 DoD Assessment Methodology

According to data available in the Electronic Data Access system for fiscal years (FYs) 2016, 2017, and 2018, on an annual basis DoD awards on average 485,859 contracts and orders that contain DFARS clause 252.204–7012 to 39,204 unique awardees, of which 262,509 awards (54 percent) are made to 26,468 small entities (68 percent). While there may be some entities that have contracts that contain the clause at 252.204–7012, but never process CUI and, therefore, do not have to implement NIST SP 800–171, it is not possible for DoD to estimate what fraction of unique entities fall into this category. Assuming all of these small entities have covered contractor information systems that are required to be in compliance with NIST SP 800–171, then all of these entities would be required to have, at minimum, a Basic Assessment in order to be considered for award.

The requirement for the Basic Assessment would be imposed through incorporation of the new solicitation provision and contract clause in new contracts and orders. As such, the requirement to have completed a Basic Assessment is expected to phase-in over a three-year period, thus impacting an estimated 8,823 small entities each year. It is expected that the Medium and High Assessments, on the other hand, will be conducted on a finite number of awardees each year based on the capacity of the Government to conduct these assessments. DoD estimates that 200 unique entities will undergo a Medium Assessment each year, of which 148 are expected to be small entities. High Assessments are expected to be conducted on approximately 110 unique entities each year, of which 81 are expected to be small entities. DoD Assessments are valid for three years, so small entities will be required to renew, at minimum, their basic assessment every three years in order to continue to receive DoD awards or to continue performance on contracts and orders with options. The following is a summary of the number of small entities that will be required to undergo NIST SP 800–171 DoD Assessments over a three-year period:

Assessment	Year 1	Year 2	Year 3
Basic	8,823	8,823	8,823
Medium	148	148	148
High	81	81	81

The top five NAICS code industries expected to be impacted by this rule are as follows: 541712, Research and Development in the Physical, Engineering, and Life Sciences (Except Biotechnology); 541330, Engineering Services; 236220, Commercial and Institutional Building Construction; 541519, Other Computer Related Services; and 561210, Facilities Support Services. These NAICS codes were selected based on a review of NAICS codes associated with awards that include the clause at DFARS 252.204–7012.

2. The CMMC Framework

Given the enterprise-wide implementation of CMMC, the Department developed a five-year phased rollout strategy. The rollout is intended to minimize the financial impacts to the industrial base, especially small entities, and disruption to the existing DoD supply chain. The Office of the Secretary of Defense staff is coordinating with the Military Services and Department Agencies to identify candidate contracts during the first five years of implementation that will include the CMMC requirement in the statement of work.

Prior to October 1, 2025, this rule impacts certain large and small businesses that are competing on acquisitions that specify a requirement for CMMC in the statement of work. These businesses will be required to have the stated CMMC certification level at the time of contract award. Inclusion of a CMMC requirement in a

solicitation during this time period must be approved by the USD(A&S). It is estimated that 129,810 unique entities will pursue their initial CMMC certification during the initial five-year period. By October 1, 2025, all entities receiving DoD contracts and orders, other than contracts or orders exclusively for commercially available off-the-shelf items or those valued at or below the micro-purchase threshold, will be required to have the CMMC Level identified in the solicitation, but which at minimum will be a CMMC Level 1 certification. CMMC certifications are valid for three years; therefore, large and small businesses will be required to renew their certification every three years.

Based on information from the Federal Procurement Data System (FPDS), the number of unique prime contractors is 212,657 and the number of known unique subcontractors is 8,309. Therefore, the total number of known unique prime contractors and subcontractors is 220,966, of which approximately 163,391 (74 percent) are estimated to be unique small businesses. According to FPDS, the average number of new contracts for unique contractors is 47,905 for any given year. The timeline required to implement CMMC across the DoD contractor population will be approximately 7 years. The phased rollout plan for years 1–7 for small entities is detailed below with the total number of unique DoD contractors and subcontractors specified. The rollout assumes that for every unique prime contractor there are approximately 100 unique subcontractors. Each small business represented in the table would be required to pursue recertification every three years in order to continue to do business with DoD.

Year	Level 1	Level 2	Level 3	Level 4	Level 5	Total
1	665	110	335	0	0	1,110
2	3,323	555	1,661	2	2	5,543
3	11,086	1,848	5,543	4	4	18,485
4	21,248	3,542	10,624	6	6	35,426
5	21,245	3,541	10,623	7	7	35,423
6	21,245	3,541	10,623	7	7	35,423
7	19,180	3,197	9,590	7	7	31,981
1–7	97,992	16,334	48,999	33	33	163,391

The top five NAICS code industries expected to be impacted by this rule are as follows: 541712, Research and Development in the Physical, Engineering, and Life Sciences (Except Biotechnology); 541330, Engineering Services; 236220, Commercial and Institutional Building Construction; 541519, Other Computer Related Services; and 561210, Facilities Support Services. These NAICS codes are the same as the DoD Assessment NAICS codes and were selected based on a review of NAICS codes associated with awards that include the clause at FAR 52.204–21 or DFARS 252.204–7012.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Rule

Details on the compliance requirements and associated costs, savings, and benefits of this rule are provided in the Regulatory Impact Analysis referenced in section IV of this preamble. The following is a summary of the compliance requirements and the estimated costs for small entities to undergo a DoD NIST SP 800–171 Assessment or obtain a CMMC certification. For both the DoD Assessment Methodology and the CMMC Framework, the estimated public costs are based on the cost for an entity to pursue each type of assessment: The Basic, Medium, or High Assessment under the DoD Assessment Methodology; or the CMMC Level 1, 2, 3, 4, or 5 certifications. The estimated costs attributed to this rule do not include the costs associated with compliance with the existing cybersecurity requirements under the clause at FAR 52.204–21 or associated with implementing NIST SP 800–171 in accordance with the clause at DFARS 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Contractors who have been awarded a DoD contract that include these existing contract clauses should have already implemented these cybersecurity requirements and incurred the associated costs; therefore, those costs are not attributed to this rule.

1. DoD Assessment Methodology

To comply with NIST SP 800–171 a company must (1) implement 110 security requirements on their covered contractor information systems; or (2) document in a "system security plan" and "plans of action" those requirements that are not yet implemented and when the requirements will be implemented. All offerors that are required to implement NIST SP 800–171 on covered contractor information systems pursuant to DFARS clause 252.204–7012, will be required to complete a Basic Assessment and upload the resulting score to the Supplier Risk Management System (SPRS), DoD's authoritative source for supplier and product performance information. The Basic Assessment is a self-assessment done by the contractor using a specific scoring methodology that tells the Department how many security requirements have not yet been implemented and is valid for three years. A company that has fully implemented all 110 NIST SP 800–171 security requirements, would have a score of 110 to report in SPRS for their Basic Assessment. A company that has unimplemented requirements will use the scoring methodology to assign a value to each unimplemented requirement, add up those values, and subcontract the total value from 110 to determine their score.

In accordance with NIST SP 800–171, a contractor should already be aware of the security requirements they have not yet implemented and have documented plans of action for those requirements; therefore, the burden associated with conducting a self-assessment is the time burden associated with calculating the score. DoD estimates that the burden to calculate the Basic Assessment score is thirty minutes per entity at a journeyman-level-2 rate of pay (0.50 hour * $99.08/hour = $49.54/assessment)).

To submit the Basic Assessment, the contractor is required to complete 6 fields: System security plan name (if more than one system is involved); CAGE code associated with the plan; a brief description of the plan architecture; date of the assessment; total score; and the date a score of 110 will be achieved. All of this data is available from the Basic Assessment itself, the existing system security plan, and the plans of action. The contractor selects the date when the last plan of

action will be complete as the date when a score of 110 will be achieved. The burden to submit a Basic Assessment for posting in SPRS is estimated to be 15 minutes per entity at a journeyman-level-2 rate of pay (0.25 hour * $99.08/hour = $24.77/assessment)). Therefore, the total cost per assessment per entity is approximately $74.31 ($49.54 + $24.77).

The estimate for the rate of pay for both preparation and submission of the Basic Assessment is journeyman-level-2, which is an employee who has the equivalent skills, responsibilities, and experience as a General Schedule (GS) 13 Federal Government employee. While these are rather simple tasks that can reasonably be completed by a GS–11 equivalent employee, or even a GS–9 clerk, the GS–13 (or perhaps GS–11) is the most likely grade for several reasons. First, in a small company, the number of IT personnel are very limited. The employee that is available to complete this task would also have significant responsibilities for operation and maintenance of the IT system and, therefore, be at a higher grade than would otherwise be required if the only job was to prepare and submit the assessment. Second, while the calculation of the assessment is simple, the personnel who would typically have access to and understand the system security plan and plans of action in order to complete the Basic Assessment would be at the higher grade. Third, while the actual submission is a simple task, the person who would complete the assessment and submit the data in SPRS would be the person with SPRS access/responsibilities, and therefore at the higher grade. Fourth, given that proper calculation of the score and its submission may well determine whether or not the company is awarded the contract, the persons preparing and submitting the report are likely to be at a higher grade than is actually required to ensure this is done properly.

After a contract is awarded, DoD may choose to conduct a Medium or High Assessment of an offer based on the criticality of the program or the sensitivity of information being handled by the contractor. Under both the Medium and High Assessment DoD assessors will be reviewing the contractor's system security plan description of how each NIST SP 800–171 requirement is met and will identify any descriptions that may not properly address the security requirements. The contractor provides DoD access to its facilities and personnel, if necessary, and prepares for/participates in the assessment conducted by the DoD. Under a High Assessment a contractor will be asked to demonstrate their system security plan. DoD will post the results in SPRS.

For the Medium Assessment, DoD estimates that the burden for a small entity to make the system security plan and supporting documentation available for review by the DoD assessor is one hour per entity at a journeyman-level-2 rate of pay, a cost of $99.08/assessment (1 hour * $99.08/hour). It is estimated that the burden for a small entity to participate in the review and discussion of the system security plan and supporting documents with the DoD assessor is three hours, with one journeyman-level-2 and one senior-level-2 contractor employee participating in the assessment, a cost of $710.40/assessment ((3 hours * $99.08/hour = $297.24) + (3 hours * $137.72/hour = $413.16)). Assuming issues are identified by the DoD Assessor, DoD estimates that the burden for a small entity to determine and provide to DoD the date by which the issues will be resolved is one hour per entity at a journeyman-level rate of pay, a cost of $99.08/assessment (1 hour * $99.08/hour). Therefore, total estimated cost for a small entity that undergoes a Medium Assessment is $908.56/assessment ($99.08 + $710.40 + $99.08).

For the High Assessment, DoD estimates that the burden for a small entity to participate in the review and discussion of the system security plan and supporting documents to the DoD assessors is 116 hours per entity at a cost of $14,542.24/assessment. The cost estimate is based on 2 senior-level-2 employees dedicating 32 hours each, 8 senior-level-1 employees dedicating 4 hours each, and 10 journeyman-level employees dedicating 2 hours each ((2 * 32 hours * $137.72/hour = $8,814.08) + (8 * 4 hours * 117.08/hour = $3,746.56) + (10 * 2 hours * $99.08/hour = 1,981.60)). It is estimated that the burden to make the system security plan and supporting documentation available for review by the DoD assessors, prepare for demonstration of requirements implementation, and to conduct post review activities is 304 hours per entity, at a cost of $36,133.76/assessment. The cost estimate is based on 2 senior-level-2 employees dedicating 48 hours each, 8 senior-level-1 employees dedicating 16 hours each, and 10 journeyman-level employees dedicating 8 hours each ((2 * 48 hours * $137.72/hour = $13,221.12) + (8 * 16 hours * 117.08/hour = $14,986.24) + (10 * 8 hours * $99.08/hour = $7,926.40)). Therefore, total estimated cost for a small entity that undergoes a High Assessment is $50,676/assessment ($14,542.24 + $36,133.76). DoD considers this to be the upper estimate of the cost, as it assumes a very robust information technology workforce. For many smaller companies, which may not have a complex information system to manage, the information system staff will be a much more limited, and labor that can be devoted (or is necessary) to prepare for and participate in the assessment is likely to be significantly less than estimated.

The following table provides the estimated annual costs for small entities to comply with the DoD Assessment requirements of this rule. Since assessments are valid for three years, the cost per assessment has been divided by three to estimate the annual cost per entity:

Assessment	Cost/ assessment	Annual cost/entity	Total unique entities	Annual cost all entities
Basic	$75	$25	26,469	$655,637
Medium	909	303	444	134,467
High	50,676	16,892	243	4,104,756
Total			27,156	4,894,860

The following table presents the average annual cost per small entity for each DoD Assessment as a percentage of the annual revenue for a small entity for four of the top five NAICS codes. The low-end of the range of annual revenues presented in the table includes the average annual revenue for smaller sized firms. The high-end of the range includes the maximum annual revenue allowed by the Small Business Administration (SBA) for a small

business, per the SBA's small business size standards published at 13 CFR 121.201. NAICS code 541712 is excluded, because it is no longer an active NAICS code and the prior size standard was based on number of employees.

NAICS code	Range of annual revenues for small businesses (in millions)	Basic assessment annual cost as % of annual revenue	Medium assessment annual cost as % of annual revenue	High assessment annual cost as % of annual revenue
541330	$5–16.5	0.0005–0.0002	0.0061–0.0018	0.3378–0.1024
236220	$10–$39.5	0.0002–0.0001	0.0030–0.0008	0.1689–0.0428
541519	$10–$30.0	0.0002–0.0001	0.0030–0.0010	0.1689–0.0563
561210	$10–$41.5	0.0002–0.0001	0.0030–0.0007	0.1689–0.0407

2. CMMC Framework

This rule adds DFARS clause 252.204–7021, Cybersecurity Maturity Model Certification Requirement, which requires the contractor to have the CMMC certification at the level required in the solicitation by contract award and maintain the required CMMC level for the duration of the contract. In order to achieve a specific CMMC level, a DIB company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

The following table provides a high-level description of the processes and practices evaluated during a CMMC assessment at each level; however, more specific information on the processes and practices associated with each CMMC Level is available at *https://www.acq.osd.mil/cmmc/index.html.*

Level	Description
1	Consists of the 15 basic safeguarding requirements from FAR clause 52.204–21.
2	Consists of 65 security requirements from NIST SP 800–171 implemented via DFARS clause 252.204–7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3.
3	Consists of all 110 security requirements from NIST SP 800–171, 20 CMMC practices, and 3 CMMC processes.
4	Consists of all 110 security requirements from NIST SP 800–171, 46 CMMC practices, and 4 CMMC processes.
5	Consists of all 110 security requirements from NIST SP 800–171, 61 CMMC practices, and 5 CMMC processes.

CMMC Assessments will be conducted by C3PAOs, which are accredited by the CMMC–AB. C3PAOs will provide CMMC Assessment reports to the CMMC–AB who will then maintain and store these reports in appropriate database(s). The CMMC–AB will issue CMMC certificates upon the resolution of any disputes or anomalies during the conduct of the assessment. These CMMC certificates will be distributed to the DIB contractor and the requisite information will be posted in SPRS.

If a contractor disputes the outcome of a C3PAO assessment, the contractor may submit a dispute adjudication request to the CMMC–AB along with supporting information related to claimed errors, malfeasance, or ethical lapses by the C3PAO. The CMMC–AB will follow a formal process to review the adjudication request and provide a preliminary evaluation to the contractor and C3PAO. If the contractor does not accept the CMMC–AB preliminary finding, the contractor may request an additional assessment by the CMMC–AB staff.

The costs associated with the preparation and the conduct of CMMC Assessments assumes that a small DIB company, in general, possesses a less complex and less expansive IT and cybersecurity infrastructure and operations relative to a larger DIB company. In estimating the cost for a small DIB company to obtain a CMMC certification, DoD took into account non-recurring engineering costs, recurring engineering costs, the cost to participate in the assessment, and re-certification costs:

- Nonrecurring engineering costs consist of hardware, software, and the associated labor. The costs are incurred only in the year of the initial assessment.
- Recurring engineering costs consist of any recurring fees and associated labor for technology refresh. The recurring engineering costs associated with technology refresh have been spread uniformly over a 5-year period (*i.e.,* 20% each year as recurring engineering costs).
- Assessment costs consist of contractor support for pre-assessment preparations, the actual assessment, and any post-assessment work. These costs also include an estimate of the potential C3PAO costs for conducting CMMC Assessment, which are comprised of labor for supporting pre-assessment preparations, actual assessment, and post-assessment work, plus travel cost.
- Re-certification costs are the same as the initial certification cost.

The following is a summary of the estimated costs for a small entity to achieve certification at each CMMC Level.

i. Level 1 Certification

Contractors pursuing a Level 1 Certification should have already implemented the 15 existing basic safeguarding requirements under FAR clause 52.204–21. Therefore, there are no estimated nonrecurring or recurring engineering costs associated with CMMC Level 1.

DoD estimates that the cost for a small entity to support a CMMC Level 1 Assessment or recertification is $2,999.56:

- *Contractor Support.* It is estimated that one journeyman-level-1 employee will dedicate 14 hours to support the assessment (8 hours for pre- and post-assessment support + 6 hours for the assessment). The estimated cost is $1,166.48 (1 journeyman * $83.32/hour * 14 hours).
- *C3PAO Assessment.* It is estimated that one journeyman-level-1 employee will dedicate 19 hours to conduct the assessment (8 hours for pre- and post-assessment support + 6 hours for the assessment + 5 hours for travel). Each employee is estimated to have 1 day of per diem for travel. The estimated cost

is $1,833.08 ((1 journeyman * $83.32/hour * 19 hours = $1,583.08) + (1 employees * 1 day * $250/day = $250 travel costs)).

ii. Level 2 Certification

Contractors pursuing a Level 2 Certification should have already implemented the 65 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation of 9 new requirements (7 CMMC practices and 2 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $8,135. The estimated recurring engineering cost per entity per year is $20,154.

DoD estimates that the cost for a small entity to support a CMMC Level 2 Assessment or recertification is $22,466.88.

- *Contractor Support.* It is estimated that two senior-level-1 employees will dedicate 48 hours each to support the assessment (24 hours for pre- and post-assessment support + 24 hours for the assessment). The estimated cost is $11,239.68 (2 senior * $117.08/hour * 48 hours).
- *C3PAO Assessment.* It is estimated that one journeyman-level-2 employee and one senior-level-1 employee will dedicate 45 hours each to conduct the assessment (16 hours for pre- and post-assessment support + 24 hours for the assessment + 5 hours for travel). Each employee is estimated to have 3 days of per diem for travel. The estimated cost is $11,227.20 ((1 senior * $117.08/hour * 45 hours = $5,268.60) + (1 journeyman * $99.08/hour * 45 hours = $4,458.60) + (2 employees * 3 days * $250/day = $1,500 travel costs)).

iii. Level 3 Certification

Contractors pursuing a Level 3 Certification should have already implemented the 110 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation 23 new requirements (20 CMMC practices and 3 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $26,214. The estimated recurring engineering cost per entity per year is $41,666.

DoD estimates that the cost for a small entity to support a CMMC Level 3 assessment or recertification is $51,095.60.

- *Contractor Support.* It is estimated that three senior-level-1 employees will dedicate 64 hours each to support the assessment (32 hours for pre- and post-assessment support + 32 hours for the assessment). The estimated cost is $22,479.36 (3 seniors * $117.08/hour * 64 hours).
- *C3PAO Assessment.* It is estimated that one senior-level-1 employee and three journeyman-level-2 employees will dedicate 57 hours each to conduct the assessment (24 hours for pre- and post-assessment support + 32 hours for the assessment + 5 hours for travel). Each employee is estimated to have 5 days of per diem for travel. The estimated cost is $28,616.24 ((1 senior * $117.08/hour * 57 hours = $6,673.56) + (3 journeyman * $99.08/hour * 57 hours = $16,942.68) + (4 employees * 5 days * $250/day = $5,000 travel costs)).

iv. Level 4 Certification

Contractors pursuing a Level 4 Certification should have already implemented the 110 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation 50 new requirements (46 CMMC practices and 4 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $938,336. The estimated recurring engineering cost per entity per year is $301,514.

DoD estimates that the cost for a small entity to support a CMMC Level 4 Assessment or recertification is $70,065.04.

- *Contractor Support.* It is estimated that three senior-level-2 employees will dedicate 80 hours each to support the assessment (40 hours for pre- and post-assessment support + 40 hours for the assessment). The estimated cost is $33,052.80 (3 seniors * $137.72/hour * 80 hours)
- *C3PAO Assessment.* It is estimated that one senior-level-2 employee and three journeyman-level-2 employees will dedicate 69 hours each to conduct the assessment (32 hours for pre- and post-assessment support + 48 hours for the assessment + 5 hours for travel). Each employee is estimated to have 5 days of per diem for travel, plus airfare. The estimated cost is $37,012.24 ((1 senior * $137.72/hour * 69 hours = $9502.68) + (3 journeyman * $99.08/hour * 69 hours = $20,509.56) + (4 employees * 5 days * $250/day = $5,000 travel costs) + (4 employees * $500 = $2,000 airfare)).

v. Level 5 Certification

Contractors pursuing a Level 5 Certification should have already implemented the 110 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation 66 new requirements (61 CMMC practices and 5 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $1,230,214. The estimated recurring engineering cost per entity per year is $384,666.

DoD estimates that the cost for a small entity to support a CMMC Level 5 Assessment or recertification is $110,090.80.

- *Contractor Support.* It is estimated that four senior-level-2 employees will dedicate 104 hours each to support the assessment (48 hours for pre- and post-assessment support + 56 hours for the assessment). The estimated cost is $57,291.52 (4 senior * $137.72/hour * 104 hours).
- *C3PAO Assessment.* It is estimated that one senior-level-2 employee, two senior-level-1 employees, and one journeyman-level-2 employee will dedicate 93 hours each to conduct the assessment (32 hours for pre- and post-assessment support + 56 hours for the assessment + 5 hours for travel). Each employee is estimated to have 7 days of per diem for travel. The estimated cost is $52,799.28 ((1 senior * $137.72/hour * 93 hours = $12,807.96) + (2 senior * $117.08/hour * 93 hours = $21,776.88) + (1 journeyman * $99.08/hour * 93 hours = $9,214.44) + (4 employees * 7 days * $250/day = $7,000 travel costs) + (4 employees * $500 = $2,000 airfare)).

vi. Total Estimated Annual Costs

The following table provides a summary of the total estimated annual costs for an individual small entity to obtain each CMMC certification level. Nonrecurring engineering costs are spread over a 20-year period to determine the average annual cost per entity. Assessment costs have been spread over a 3-year period, since entities will participate in a reassessment every 3 years.

CMMC cert	Average nonrecurring engineering costs	Recurring engineering costs	Average assessment costs	Total annual assessment cost
Level 1	$0	$0	$1,000	$1,000

CMMC cert	Average nonrecurring engineering costs	Recurring engineering costs	Average assessment costs	Total annual assessment cost
Level 2	407	20,154	7,489	28,050
Level 3	1,311	41,666	17,032	60,009
Level 4	46,917	301,514	23,355	371,786
Level 5	61,511	384,666	36,697	482,874

The following table presents the average annual cost per small entity for CMMC certifications at levels 1 through 3 as a percentage of the annual revenue for a small entity for four of the top five NAICS codes. The low-end of the range of annual revenues presented in the table includes the average annual revenue for smaller sized firms. The high-end of the range includes the maximum annual revenue allowed by the SBA for a small business, per the SBA's small business size standards published at 13 CFR 121.201. NAICS code 541712 is excluded, because it is no longer an active NAICS code and the prior size standard was based on number of employees.

NAICS code	Range of annual revenues for small businesses (in millions)	CMMC level 1 annual cost as % of annual revenue	CMMC level 2 annual cost as % of annual revenue	CMMC level 3 annual cost as % of annual revenue
541330	$5–$16.5	0.0200–0.0061	0.5610–0.1700	1.2002–0.3637
236220	$10–$39.5	0.0100–0.0025	0.2805–0.0710	0.6001–0.1519
541519	$10–$30.0	0.0100–0.0033	0.2805–0.0935	0.6001–0.2000
561210	$10–$41.5	0.0100–0.0024	0.2805–0.0676	0.6001–0.1446

For CMMC certification at levels 4 and 5, the following table presents the annual cost per small entity for CMMC certification at levels 4 and 5 as a percentage of the low, average, and high annual revenues for entities that have represented themselves as small in the System for Award Management (SAM) for their primary NAICS code and are performing on contracts that could be subject to a CMMC level 4 or 5 certification requirements. The values of the low, average, and high annual revenues are based on an average of the annual receipt reported in SAM by such entities for FY16 through FY20.

FY16 thru FY20	Annual revenue of entities represented as small for primary NAICS	Level 4 certification cost as % of annual revenue	Level 5 certification cost as % of annual revenue
Low	$6.5 million	5.67	7.36
Average	$22.9 million	1.62	2.11
High	$85 million	0.43	0.56

The following is a summary of the estimated annual costs in millions for all 163,391 small entities to achieve their initial CMMC certifications (and recertifications every three years) over a 10-year period:

Year	Level 1	Level 2	Level 3	Level 4	Level 5
1	$1.99	$5.58	$39.86	$0.00	$0.00
2	9.97	30.39	211.58	2.62	3.45
3	33.25	107.20	742.65	5.84	7.67
4	65.73	232.90	1,595.23	9.67	12.66
5	73.69	314.23	2,105.53	12.93	16.91
6	96.98	414.64	2,746.50	15.18	19.82
7	123.26	509.08	3,342.95	17.43	22.74
8	73.69	421.22	2,669.25	10.58	13.68
9	96.98	450.27	2,867.60	10.72	13.90
10	123.26	483.07	3,091.56	10.86	14.13

E. Relevant Federal Rules, Which May Duplicate, Overlap, or Conflict With the Rule

The rule does not duplicate, overlap, or conflict with any other Federal rules. Rather this rule validates and verifies contractor compliance with the existing cybersecurity requirements in FAR clause 52.204–21 and DFARS clause 252.204–7012, and ensures that the entire DIB sector has the appropriate cybersecurity processes and practices in place to properly protect FCI and CUI during performance of DoD contracts.

F. Description of Any Significant Alternatives to the Rule Which Accomplish the Stated Objectives of Applicable Statutes and Which Minimize Any Significant Economic Impact of the Rule on Small Entities

DoD considered and adopted several alternatives during the development of

this rule that reduce the burden on small entities and still meet the objectives of the rule. These alternatives include: (1) Exempting contracts and orders exclusively for the acquisition of commercially available off-the-shelf items; and (2) implementing a phased rollout for the CMMC portion of the rule and stipulating that the inclusion a CMMC requirement in new contracts until that time be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment. Additional alternatives were considered, however, it was determined that these other alternatives did not achieve the intended policy outcome.

1. CMMC Model and Implementation

The Regulatory Impact Analysis (RIA) referenced in section IV of this preamble estimates that the total number of unique DoD contractors and subcontractors is 220,966, with approximately 163,391 or 74% being small entities. The RIA also specifies the estimates for the percentage of all contractors and subcontractors associated with each CMMC level. These estimates indicate that the vast majority of small entities (*i.e.,* 163,325 of 163,391 or 99.96%) will be required to achieve CMMC Level 1–3 certificates during the initial rollout. The Department looked at Levels 1 through 5 to determine if there were alternatives and whether these alternatives met the intended policy outcome.

For CMMC Level 1, the practices map directly to the basic safeguarding requirements specified in the clause at FAR 52.204–21. The phased rollout estimates that the majority of small entities (*i.e.,* 97,992 of the 163,325 or 60%) will be required to achieve CMMC Level 1. The planned implementation of CMMC Level 1 adds a verification component to the existing FAR clause by including an on-site assessment by a credentialed assessor from an accredited C3PAO. The on-site assessment verifies the implementation of the required cybersecurity practices and further supports the physical identification of contractors and subcontractors in the DoD supply chain. In the aggregate, the estimated cost associated with supporting this on-site assessment and approximated C3PAO fees does not represent a cost-driver with respect to CMMC costs to small entities across levels. An alternative to an on-site assessment is for contractors to provide documentation and supporting evidence of the proper implementation of the required cybersecurity practices through a secure online portal. These artifacts would then be reviewed and checked virtually by an accredited assessor prior to the CMMC–AB issuing a CMMC Level 1 certificate. The drawback of this alternative is the inability of the contractor to interact with the C3PAO assessor in person and provide evidence directly without transmitting proprietary information. Small entities will not receive as much meaningful and interactive feedback that would be part of a Level 1 on-site assessment.

For CMMC Level 2, the practices encompass only 48 of the 110 security requirements of NIST SP 800–171, as specified in DFARS clause 252.204–7012, and 7 additional cybersecurity requirements. In addition, CMMC Level 2 includes two process maturity requirements. The phased rollout estimates that approximately 10% of small entities may choose to use Level 2 as a transition step from Level 1 to Level 3. Small entities that achieve Level 1 can seek to achieve Level 3 (without first achieving a Level 2 certification) if the necessary cybersecurity practices and processes have been implemented. The Department does not anticipate releasing new contracts that require contractors to achieve CMMC Level 2. As a result, the Department did not consider alternatives with respect to CMMC Level 2.

For CMMC Level 3, the practices encompass all the 110 security requirements of NIST SP 800–171, as specified in DFARS clause 252.204–7012, as well as 13 additional cybersecurity requirements above Level 2. In addition, CMMC Level 3 includes three process maturity requirements. These additional cybersecurity practices were incorporated based upon several considerations that included public comments from September to December 2019 on draft versions of the model, inputs from the DIB Sector Coordinating Council (SCC), cybersecurity threats, the progression of cybersecurity capabilities from Level 3 to Levels 4, and other factors. The CMMC phased rollout estimates that 48,999 of the 163,325 small entities or 30% will be required to achieve CMMC Level 3. The alternatives considered include removing a subset or all of the 20 additional practices at Level 3 or moving a subset or all of the 20 additional practices from Level 3 to Level 4. The primary drawback of these alternatives is that the cybersecurity capability gaps associated with protecting CUI will not be addressed until Level 4, which will apply to a relatively small percentage of non-small and small entities. Furthermore, the progression of cybersecurity capabilities from Level 3 to Level 4 becomes more abrupt.

For CMMC Level 4, the practices encompass the 110 security requirements of NIST SP 800–171 as specified in DFARS clause 252.204–7012 and 46 additional cybersecurity requirements. More specifically, CMMC Level 4 adds 26 enhanced security requirements above CMMC Level 3, of which 13 are derived from Draft NIST SP 800–171B. In addition, CMMC Level 4 includes four process maturity requirements. The DIB SCC and the public contributed to the specification of the other 13 enhanced security requirements. For CMMC Level 4, an alternative considered is to define a threshold for contractors to meet 15 out of the 26 enhanced security requirements. In addition, contractors will be required to meet 6 out of the 11 remaining non-threshold enhanced security requirements. This alternative implies that a contractor will have to implement 21 of the 26 enhanced security requirements as well as the associated maturity processes. A drawback of this alternative is that contractors implement a different subset of the 11 non-threshold requirements which in turn, leads to a non-uniform set of cybersecurity capabilities across those certified at Level 4.

For CMMC Level 5, the practices encompass the 110 security requirements of NIST SP 800–171 as specified in DFARS clause 252.204–7012 and 61 additional cybersecurity requirements. More specifically, CMMC Level 5 adds 15 enhanced security requirements above CMMC Level 4, of which 4 are derived from Draft NIST SP 800–171B. In addition, CMMC Level 5 includes five process maturity requirements. The DIB SCC and the public contributed to the specification of the other 11 enhanced security requirements. For CMMC Level 5, the alternative considered is to define a threshold for contractors to meet 6 out of the 15 enhanced security requirements. In addition, contractors will be required to meet 5 out of the 9 remaining non-threshold enhanced security requirements. This alternative implies that a contractor will have implemented 11 of the 15 enhanced security requirements as well as the associated maturity processes. A drawback of this alternative is that contractors implement a different subset of the 9 non-threshold requirements which in turn, leads to a non-uniform set of cybersecurity capabilities across those certified at Level 5.

2. Timing of CMMC Level Certification Requirement

In addition to evaluating the make-up of the CMMC levels, the Department

took into consideration the timing of the requirement to achieve a CMMC level certification: (1) At time of proposal or offer submission, (2) in order to receive award, or (3) post contract award. The Department ultimately adopted alternative 2 to require certification at the time of award. The drawback of alternative 1 (at time of proposal or offer submission) is the increased risk for contractors since they may not have sufficient time to achieve the required CMMC certification after the release of the Request for Information (RFI). The drawback of alternative 3 (after contract award) is the increased risk to the Department with respect to the schedule and uncertainty with respect to the case where the contractor is unable to achieve the required CMMC level in a reasonable amount of time given their current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI. The Department seeks public comment on the timing of contract award, to include the effect of requiring certification at time of award on small businesses.

DoD invites comments from small business concerns and other interested parties on the expected impact of this rule on small entities. DoD will also consider comments from small entities concerning the existing regulations in subparts affected by this rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (DFARS Case 2019–D041), in correspondence.

VIII. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information, unless that collection has obtained OMB approval and displays a currently valid OMB Control Number.

DoD requested, and OMB authorized, emergency processing of the collection of information tied to this rule, as OMB Control Number 0750–0004, *Assessing Contractor Implementation of Cybersecurity Requirements,* consistent with 5 CFR 1320.13.

DoD has determined the following conditions have been met:

a. The collection of information is needed prior to the expiration of time periods normally associated with a routine submission for review under the provisions of the PRA, to enable the Department to immediately begin assessing the current status of contractor implementation of NIST SP 800–171 on their information systems that process CUI.

b. The collection of information is essential to DoD's mission. The collection of information is essential to DoD's mission. The National Defense Strategy (NDS) and DoD Cyber Strategy highlight the importance of protecting the Defense Industrial Base (DIB) to maintain national and economic security. To this end, DoD requires defense contractors and subcontractors to implement the NIST SP 800–171 security requirements on information systems that handle CUI, pursuant to DFARS clause 252.204–7012. This DoD Assessment Methodology enables the Department to assess strategically, at a corporate-level, contractor implementation of the NIST SP 800–171 security requirements. Results of a NIST SP 800–171 DoD Assessment reflect the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor.

c. Moreover, DoD cannot comply with the normal clearance procedures, because public harm is reasonably likely to result if current clearance procedures are followed. Authorizing collection of this information on the effective date will motivate defense contractors and subcontractors who have not yet implemented existing NIST SP 800–171 security requirements, to take action to implement the security requirements on covered information systems that process CUI, in order to protect our national and economic security interests. The aggregate loss of sensitive controlled unclassified information and intellectual property from the DIB sector could undermine U.S. technological advantages and increase risk to DoD missions.

Upon publication of this rule, DoD intends to provide a separate 60-day notice in the **Federal Register** requesting public comment for OMB Control Number 0750–0004, *Assessing Contractor Implementation of Cybersecurity Requirements.*

DOD estimates the annual public reporting burden for the information collection as follows:

a. Basic Assessment

Respondents: 13,068.
Responses per respondent: 1.
Total annual responses: 13,068.
Hours per response: .75.
Total burden hours: 9,801.

b. Medium Assessment

Respondents: 200.
Responses per respondent: 1.
Total annual responses: 200.
Hours per response: 8.
Total burden hours: 1,600.

c. High Assessment

Respondents: 110.
Responses per respondent: 1.
Total annual responses: 110.
Hours per response: 420.
Total burden hours: 46,200.

d. Total Public Burden (All Entities)

Respondents: 13,068.
Total annual responses: 13,378.
Total burden hours: 57,601.

e. Total Public Burden (Small Entities)

Respondents: 8,823.
Total annual responses: 9,023.
Total burden hours: 41,821.

The requirement to collect information from offerors and contractors regarding the status of their implementation of NIST SP 800–171 on their information systems that process CUI, is being imposed via a new solicitation provision and contract clause. Per the new provision, if an offeror is required to have implemented the NIST SP 800–171 security requirements on their information systems pursuant to DFARS clause 252.204–7012, then the offeror must have, at minimum, a current self-assessment (or Basic Assessment) uploaded to DoD's Supplier Performance Risk System, in order to be considered for award. Depending on the criticality of the acquisition program, after contract award, certain contractors may be required to participate in a Medium or High assessment to be conducted by DoD assessor. During these post-award assessments, contractors will be required to demonstrate their implementation of NIST SP 800–171 security requirements. Results of a NIST SP 800–171 DoD Assessment reflect the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor.

IX. Determination To Issue an Interim Rule

A determination has been made under the authority of the Secretary of Defense that urgent and compelling reasons exist to promulgate this interim rule without prior opportunity for public comment pursuant to 41 U.S.C. 1707(d) and FAR 1.501–3(b).

Malicious cyber actors have targeted, and continue to target, the DIB sector, which consists of over 200,000 small-to-large sized entities that support the warfighter. In particular, actors ranging from cyber criminals to nation-states continue to attack companies and organizations that comprise the Department's multi-tier supply chain including smaller entities at the lower

tiers. These actors seek to steal DoD's intellectual property to undercut the United States' strategic and technological advantage and to benefit their own military and economic development.

The Department has been focused on improving the cyber resiliency and security of the DIB sector for over a decade as evidenced by the development of minimum cybersecurity standards and the implementation of those standards in the National Institute of Standards and Technology (NIST) Special Publications (SP) and implementation of those standards in the FAR and DFARS. In 2013, DoD issued a final DFARS rule (78 FR 69273) that required contractors to implement a select number of security measures from NIST SP 800–53, Recommended Security Controls for Federal Information Systems and Organizations, to facilitate safeguarding unclassified DoD information within contractor information systems from unauthorized access and disclosure. In 2015, DoD issued an interim DFARS rule (80 FR 81472) requiring contractors that handle Controlled Unclassified Information (CUI) on their information systems to transition by December 31, 2017, from NIST SP 800–53 to NIST SP 800–171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. NIST SP 800–171 was not only easier to use, but also provided security requirements that greatly increases the protections of Government information in contractor information systems once implemented. And, in 2016, the FAR Council mandated the use of FAR clause 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, to require all Government contractors to implement, at minimum, some basic policies and practices to safeguard Federal Contract Information (FCI) within their information systems. Since then, the Department has been engaging with industry on improving their compliance with these exiting cybersecurity requirements and developing a framework to institutionalize cybersecurity process and practices throughout the DIB sector.

Notwithstanding the fact that these minimum cybersecurity standards have been in effect on DoD contracts since as early as 2013, several surveys and questionnaires by defense industrial associations have highlighted the DIB sector's continued challenges in achieving broad implementation of these security requirements. In a 2017 questionnaire, contractors and subcontractors that responded acknowledged implementation rates of 38% to 54% for at least 10 of the 110 security requirements of NIST SP 800–171.[1] In a separate 2018 survey, 36% of contractors who responded indicated a lack of awareness of DFARS clause 252.204–7012 and 45% of contractors acknowledged not having read NIST SP 800–171.[2] In a 2019 survey, contractors that responded rated their level of preparedness for a Defense Contract Management Agency standard assessment of contractor implementation of NIST SP 800–171 at 56%.[3] Furthermore, for the High Assessments conducted on-site by DoD to date, only 36% of contractors demonstrated implementation of all 110 of the NIST SP 800–171 security requirements.

Although these industry surveys represent a small sample of the DIB sector, the results were reinforced by the findings from DoD Inspector General report in 2019 (DODIG–2019–105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take immediate steps to assess a contractor's ability to protect this information. The report emphasizes that malicious actors can exploit the vulnerabilities of contractors' networks and systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies.

Defense contractors must begin viewing cybersecurity as a part of doing business, in order to protect themselves and to protect national security. The various industry surveys and Government assessments conducted to date illustrate the following: Absent a requirement for defense contractors to demonstrate implementation of standard cybersecurity processes and practices, cybersecurity requirements will not be fully implemented, leaving DoD and the DIB unprotected and vulnerable to malicious cyber activity. To this end, section 1648 of the NDAA for FY 2020 (Pub. L. 116–92) directed the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. defense industrial base no later than February 1, 2020. In the Senate Armed Services Committee Report to accompany the NDAA for FY 2020, the Committee expressed concern that DIB contractors are an inviting target for our adversaries, who have been conducting cyberattacks to steal critical military technologies.

Developing a framework to enhance the cybersecurity of the defense industrial base will serve as an important first step toward securing the supply chain. Pursuant to section 1648, DoD has developed the CMMC Framework, which gives the Department a mechanism to certify the cyber posture of its largest defense contractors to the smallest firms in our supply chain, who have become primary targets of malicious cyber activity.

This rule is an important part of the cybersecurity framework,[4] and builds on the existing FAR and DFARS clause cybersecurity requirements by (1) adding a mechanism to immediately begin assessing the current status of contractor implementation of NIST SP 800–171 on their information systems that process CUI; and (2) to require contractors and subcontractors to take steps to fully implement existing cybersecurity requirements, plus additional processes and practices, to protect FCI and CUI on their information systems in preparation for verification under the CMMC Framework. There is an urgent need for DoD to immediately begin assessing where vulnerabilities in its supply chain exist and take steps to correct such deficiencies, which can be accomplished by requiring contractors and subcontractors that handle DoD CUI on their information systems to complete a NIST SP 800–171 Basic Assessment. In fact, while this rule includes a delayed effective date, contractors and subcontractors that are required to implement NIST SP 800–171 pursuant to DFARS clause 252.204–7012, are encouraged to immediately conduct and submit a self-assessment as described in this rule to facilitate the Department's assessment.

It is equally urgent for the Department to ensure DIB contractors that have not fully implemented the basic safeguarding requirements under FAR clause 52.204–21 or the NIST SP 800–171 security requirements pursuant to DFARS 252.204–7012 begin correcting these deficiencies immediately. These are cybersecurity requirements contractors and subcontractors should have already implemented (or in the

[1] Aerospace Industries Association. "Complying with NIST 800–171." Fall 2017.

[2] National Defense Industrial Association (NDIA). "Implementing Cybersecurity in DoD Supply Chains." White Paper. July 2018.

[3] NDIA. "Beyond Obfuscation: The Defense Industry's Position within Federal Cybersecurity Policy." A Report of the NDIA Policy Department. October 2018. Page 20 and page 24.

[4] Section 1648 of the NDAA for FY 2020 mandates the formulation of "unified cybersecurity . . . regulations . . . to be imposed on the defense industrial base for the purpose of assessing the cybersecurity of individual contractors,"

case of implementation of NIST SP 800–171, have plans of action to correct deficiencies) on information systems that handle CUI. Under the CMMC Framework, a contractor is able to achieve CMMC Level 1 Certification if they can demonstrate implementation of the basic safeguarding requirements in the FAR clause. Similarly, a contractor is able to achieve CMMC Level 3 if they can demonstrate implementation of the NIST SP 800–171 security requirements, plus some additional processes and practices. This rule ensures contractors and subcontractors focus on full implementation of existing cybersecurity requirements on their information systems and expedites the Department's ability to secure its supply chain.

For the foregoing reasons, pursuant to 41 U.S.C. 1707(d), DoD finds that urgent and compelling circumstances make compliance with the notice and comment requirements of 41 U.S.C. 1707(a) impracticable, and invokes the exception to those requirements under 41 U.S.C. 1707(d) and FAR 1.501–3(b).[5] While a public comment process will not be completed prior to the rule's effective date, DoD has incorporated feedback solicited through extensive outreach already undertaken pursuant to section 1648(d) of the NDAA for FY 2020, including through public meetings and extensive industry outreach conducted over the past year. However, pursuant to 41 U.S.C. 1707 and FAR 1.501–3(b), DoD will consider public comments received in response to this interim rule in the formation of the final rule.

List of Subjects in 204, 212, 217, and 252

Government procurement.

Jennifer D. Johnson,

Regulatory Control Officer, Defense Acquisition Regulations System.

Therefore, 48 CFR parts 204, 212, 217, and 252 are amended as follows:

■ 1. The authority citation for 48 CFR parts 204, 212, 217, and 252 continues to read as follows:

Authority: 41 U.S.C. 1303 and 48 CFR chapter 1.

[5] FAR 1.501–3(b) states that "[a]dvance comments need not be solicited when urgent and compelling circumstances make solicitation of comments impracticable prior to the effective date of the coverage, such as when a new statute must be implemented in a relatively short period of time. In such case, the coverage shall be issued on a temporary basis and shall provide for at least a 30 day public comment period."

PART 204—ADMINISTRATIVE MATTERS

■ 2. Amend section 204.7302 by revising paragraph (a) to read as follows:

204.7302 Policy.

(a)(1) Contractors and subcontractors are required to provide adequate security on all covered contractor information systems.

(2) Contractors required to implement NIST SP 800–171, in accordance with the clause at 252.204–7012, Safeguarding Covered Defense Information and Cyber incident Reporting, are required at time of award to have at least a Basic NIST SP 800–171 DoD Assessment that is current (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204–7019).

(3) The NIST SP 800–171 DoD Assessment Methodology is located at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

(4) High NIST SP 800–171 DoD Assessments will be conducted by Government personnel using NIST SP 800–171A, "Assessing Security Requirements for Controlled Unclassified Information."

(5) The NIST SP 800–171 DoD Assessment will not duplicate efforts from any other DoD assessment or the Cybersecurity Maturity Model Certification (CMMC) (see subpart 204.75), except for rare circumstances when a re-assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance.

* * * * *

■ 3. Revise section 204.7303 to read as follows:

204.7303 Procedures.

(a) Follow the procedures relating to safeguarding covered defense information at PGI 204.7303.

(b) The contracting officer shall verify that the summary level score of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old, unless a lesser time is specified in the solicitation) (see 252.204–7019) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted in Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*), prior to—

(1) Awarding a contract, task order, or delivery order to an offeror or contractor that is required to implement NIST SP 800–171 in accordance with the clause at 252.204–7012; or

(2) Exercising an option period or extending the period of performance on a contract, task order, or delivery order with a contractor that is that is required to implement the NIST SP 800–171 in accordance with the clause at 252.204–7012.

■ 4. Amend section 204.7304 by revising the section heading and adding paragraphs (d) and (e) to read as follows:

204.7304 Solicitation provisions and contract clauses.

* * * * *

(d) Use the provision at 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(e) Use the clause at 252.204–7020, NIST SP 800–171 DoD Assessment Requirements, in all solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for those that are solely for the acquisition of COTS items.

■ 5. Add subpart 204.75, consisting of 204.7500 through 204.7503, to read as follows:

Subpart 204.75—Cybersecurity Maturity Model Certification

Sec.

Subpart 204.75—Cybersecurity Maturity Model Certification

204.7500 Scope of subpart.

(a) This subpart prescribes policies and procedures for including the Cybersecurity Maturity Model Certification (CMMC) level requirements in DoD contracts. CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see *https://www.acq.osd.mil/cmmc/index.html*).

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information,

nor does it affect requirements of the National Industrial Security Program.

204.7501 Policy.

(a) The contracting officer shall include in the solicitation the required CMMC level, if provided by the requiring activity. Contracting officers shall not award a contract, task order, or delivery order to an offeror that does not have a current (*i.e.,* not more than 3 years old) CMMC certificate at the level required by the solicitation.

(b) Contractors are required to achieve, at time of award, a CMMC certificate at the level specified in the solicitation. Contractors are required to maintain a current (*i.e.,* not more than 3 years old) CMMC certificate at the specified level, if required by the statement of work or requirement document, throughout the life of the contract, task order, or delivery order. Contracting officers shall not exercise an option period or extend the period of performance on a contract, task order, or delivery order, unless the contract has a current (*i.e.,* not more than 3 years old) CMMC certificate at the level required by the contract, task order, or delivery order.

(c) The CMMC Assessments shall not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a re-assessment may be necessary such as, but not limited to when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.

204.7502 Procedures.

(a) When a requiring activity identifies a requirement for a contract, task order, or delivery order to include a specific CMMC level, the contracting officer shall not—

(1) Award to an offeror that does not have a CMMC certificate at the level required by the solicitation; or

(2) Exercise an option or extend any period of performance on a contract, task order, or delivery order unless the contractor has a CMMC certificate at the level required by the contract.

(b) Contracting officers shall use Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) to verify an offeror or contractor's CMMC level.

204.7503 Contract clause.

Use the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, as follows:

(a) Until September 30, 2025, in solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf (COTS) items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement a phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by OUSD(A&S).

(b) On or after October 1, 2025, in all solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items.

PART 212—ACQUISITION OF COMMERCIAL ITEMS

■ 6. Amend section 212.301, by adding paragraphs (f)(ii)(K), (L), and (M) to read as follows:

212.301 Solicitation provisions and contract clauses for acquisition of commercial items.

* * * * *

(f) * * *

(ii) * * *

(K) Use the provision at 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements, as prescribed in 204.7304(d).

(L) Use the clause at 252.204–7020, NIST SP 800–171 DoD Assessment Requirements, as prescribed in 204.7304(e).

(M) Use the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, as prescribed in 204.7503(a) and (b).

* * * * *

PART 217—SPECIAL CONTRACTING METHODS

■ 7. Amend section 217.207 by revising paragraph (c) to read as follows:

217.207 Exercise of options.

(c) In addition to the requirements at FAR 17.207(c), exercise an option only after:

(1) Determining that the contractor's record in the System for Award Management database is active and the contractor's Data Universal Numbering System (DUNS) number, Commercial and Government Entity (CAGE) code, name, and physical address are accurately reflected in the contract document. See PGI 217.207 for the requirement to perform cost or price analysis of spare parts prior to exercising any option for firm-fixed-price contracts containing spare parts.

(2) Verifying in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) that—

(i) The summary level score of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old, unless a lesser time is specified in the solicitation) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted (see 204.7303).

(ii) The contractor has a CMMC certificate at the level required by the contract, and that it is current (*i.e.,* not more than 3 years old) (see 204.7502).

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 8. Add sections 252.204–7019, 252.204–7020, and 252.204–7021 to read as follows:

Sec.

* * * * *

252.204–7019 Notice of NIST SP 800–171 DoD Assessment Requirements.

252.204–7020 NIST SP 800–171 DoD Assessment Requirements.

252.204–7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.

* * * * *

252.204–7019 Notice of NIST SP 800–171 DoD Assessment Requirements.

As prescribed in 204.7304(d), use the following provision:

NOTICE OF NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)

(a) *Definitions.*

Basic Assessment, Medium Assessment, and *High Assessment* have the meaning given in the clause 252.204–7020, NIST SP 800–171 DoD Assessments.

Covered contractor information system has the meaning given in the clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this solicitation.

(b) *Requirement.* In order to be considered for award, if the Offeror is required to implement NIST SP 800–171, the Offeror shall have a current assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204–7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800–171 DoD Assessments are described in the NIST SP 800–171 DoD Assessment Methodology located at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

(c) *Procedures.* (1) The Offeror shall verify that summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is

specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) for all covered contractor information systems relevant to the offer.

(2) If the Offeror does not have summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the Offeror may conduct and submit a Basic Assessment to *webptsmh@navy.mil* for posting to SPRS in the format identified in paragraph (d) of this provision.

(d) *Summary level scores.* Summary level scores for all assessments will be posted 30 days post-assessment in SPRS to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments.* An Offeror may follow the procedures in paragraph (c)(2) of this provision for posting Basic Assessments to SPRS.

(i) The email shall include the following information:

(A) Cybersecurity standard assessed (*e.g.,* NIST SP 800–171 Rev 1).

(B) Organization conducting the assessment (*e.g.,* Contractor self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and

(*2*) A brief description of the system security plan architecture, if more than one plan exists.

(D) Date the assessment was completed.

(E) Summary level score (*e.g.,* 95 out of 110, NOT the individual value for each requirement).

(F) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(ii) If multiple system security plans are addressed in the email described at paragraph (d)(1)(i) of this section, the Offeror shall use the following format for the report:

System security plan	CAGE codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total score	Date score of 110 will achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system assessed:

(i) The standard assessed (*e.g.,* NIST SP 800–171 Rev 1).

(ii) Organization conducting the assessment, *e.g.,* DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) A brief description of the system security plan architecture, if more than one system security plan exists.

(v) Date and level of the assessment, *i.e.,* medium or high.

(vi) Summary level score (*e.g.,* 105 out of 110, not the individual value assigned for each requirement).

(vii) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(3) *Accessibility.* (i) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(ii) Authorized representatives of the Offeror for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.*

(iii) A High NIST SP 800–171 DoD Assessment may result in documentation in addition to that listed in this section. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (*e.g.,* Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(End of provision)

252.204–7020 NIST SP 800–171 DoD Assessment Requirements.

As prescribed in 204.7304(e), use the following clause:

NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)

(a) *Definitions.*

Basic Assessment means a contractor's self-assessment of the contractor's implementation of NIST SP 800–171 that—

(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);

(2) Is conducted in accordance with the NIST SP 800–171 DoD Assessment Methodology; and

(3) Results in a confidence level of "Low" in the resulting score, because it is a self-generated score.

Covered contractor information system has the meaning given in the clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

High Assessment means an assessment that is conducted by Government personnel using NIST SP 800–171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review;

(iii) Verification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800–171 security requirements have been implemented as described in the contractor's system security plan; and

(iv) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "High" in the resulting score.

Medium Assessment means an assessment conducted by the Government that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review; and

(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "Medium" in the resulting score.

(b) *Applicability.* This clause applies to covered contractor information systems that are required to comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, in accordance with Defense Federal Acquisition Regulation System (DFARS) clause at 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

(c) *Requirements.* The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800–171 DoD Assessment, as described in NIST SP 800–171 DoD Assessment Methodology at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html,* if necessary.

(d) *Procedures.* Summary level scores for all assessments will be posted in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) to provide DoD

Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments.* A contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800–171 DoD Assessment Methodology to *webptsmh@navy.mil* for posting to SPRS.

(i) The email shall include the following information:

(A) Version of NIST SP 800–171 against which the assessment was conducted.

(B) Organization conducting the assessment (*e.g.*, Contractor self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and

(*2*) A brief description of the system security plan architecture, if more than one plan exists.

(D) Date the assessment was completed.

(E) Summary level score (*e.g.*, 95 out of 110, NOT the individual value for each requirement).

(F) Date that all requirements are expected to be implemented (*i.e.*, a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(ii) If multiple system security plans are addressed in the email described at paragraph (b)(1)(i) of this section, the Contractor shall use the following format for the report:

System security plan	CAGE codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total score	Date score of 110 will achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system security plan assessed:

(i) The standard assessed (*e.g.*, NIST SP 800–171 Rev 1).

(ii) Organization conducting the assessment, *e.g.*, DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) A brief description of the system security plan architecture, if more than one system security plan exists.

(v) Date and level of the assessment, *i.e.*, medium or high.

(vi) Summary level score (*e.g.*, 105 out of 110, not the individual value assigned for each requirement).

(vii) Date that all requirements are expected to be implemented (*i.e.*, a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(e) *Rebuttals.* (1) DoD will provide Medium and High Assessment summary level scores to the Contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS (see SPRS User's Guide *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf*).

(2) Upon completion of each assessment, the contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

(f) *Accessibility.* (1) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(2) Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf*.

(3) A High NIST SP 800–171 DoD Assessment may result in documentation in addition to that listed in this clause. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (*e.g.*, Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(g) *Subcontracts.* (1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).

(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800–171 security requirements, in accordance with DFARS clause 252.204–7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800–171 DoD Assessment, as described in *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html*, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

(3) If a subcontractor does not have summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.*, not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800–171 DoD Assessment Methodology, to *webptsmh@navy.mil* for posting to SPRS along with the information required by paragraph (d) of this clause.

(End of clause)

252.204–7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.

As prescribed in 204.7503(a) and (b), insert the following clause:

CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENT (NOV 2020)

(a) *Scope.* The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see *https://www.acq.osd.mil/cmmc/index.html*).

(b) *Requirements.* The Contractor shall have a current (*i.e.* not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

(c) *Subcontracts.* The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (*i.e.*, not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

(End of clause)

[FR Doc. 2020–21123 Filed 9–28–20; 8:45 am]

BILLING CODE 5001–06–P

252.204-7020 NIST SP 800-171 DoD Assessment Requirements.

As prescribed in 204.7304 (e), use the following clause:

NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)

(a) *Definitions*.

Basic Assessment" means a contractor's self-assessment of the contractor's implementation of NIST SP 800-171 that—

(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);

(2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and

(3) Results in a confidence level of "Low" in the resulting score, because it is a self-generated score.

"Covered contractor information system" has the meaning given in the clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

"High Assessment" means an assessment that is conducted by Government personnel using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review;

(iii) Verification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800-171 security requirements have been implemented as described in the contractor's system security plan; and

(iv) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "High" in the resulting score.

"Medium Assessment" means an assessment conducted by the Government that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review; and

(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "Medium" in the resulting score.

(b) *Applicability*. This clause applies to covered contractor information systems that are required to comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, in accordance with Defense Federal Acquisition Regulation System (DFARS) clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

(c) *Requirements*. The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in NIST SP 800-171 DoD Assessment Methodology at https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, if necessary.

(d) *Procedures*. Summary level scores for all assessments will be posted in the Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/) to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments*. A contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology to mailto:webptsmh@navy.mil for posting to SPRS.

(i) The email shall include the following information:

(A) Version of NIST SP 800-171 against which the assessment was conducted.

(B) Organization conducting the assessment (e.g., Contractor self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and

(*2*) A brief description of the system security plan architecture, if more than one plan exists.

(D) Date the assessment was completed.

(E) Summary level score (e.g., 95 out of 110, NOT the individual value for each requirement).

(F) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(ii) If multiple system security plans are addressed in the email described at paragraph (b)(1)(i) of this section, the Contractor shall use the following format for the report:

System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total Score	Date score of 110 will achieved

(2) Medium and High Assessments. DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system security plan assessed:

(i) The standard assessed (e.g., NIST SP 800-171 Rev 1).

(ii) Organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) A brief description of the system security plan architecture, if more than one system security plan exists.

(v) Date and level of the assessment, i.e., medium or high.

(vi) Summary level score (e.g., 105 out of 110, not the individual value assigned for each requirement).

(vii) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(e) *Rebuttals*.

(1) DoD will provide Medium and High Assessment summary level scores to the Contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS (see SPRS User's Guide https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf).

(2) Upon completion of each assessment, the contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

(f) *Accessibility*.

(1) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(2) Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.

(3) A High NIST SP 800-171 DoD Assessment may result in documentation in addition to that listed in this clause. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(g) Subcontracts.

(1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).

(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

(3) If a subcontractor does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800-171 DoD Assessment Methodology, to mailto:webptsmh@navy.mil for posting to SPRS along with the information required by paragraph (d) of this clause.

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204, 212, 217, and 252

[Docket DARS–2020–0034]

RIN 0750–AJ81

Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Interim rule.

SUMMARY: DoD is issuing an interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain.

DATES: Effective November 30, 2020.

Comments on the interim rule should be submitted in writing to the address shown below on or before November 30, 2020, to be considered in the formation of a final rule.

ADDRESSES: Submit comments identified by DFARS Case 2019–D041, using any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Search for "DFARS Case 2019–D041". Select "Comment Now" and follow the instructions provided to submit a comment. Please include "DFARS Case 2019–D041" on any attached documents.
- *Email: osd.dfars@mail.mil.* Include DFARS Case 2019–D041 in the subject line of the message.

Comments received generally will be posted without change to *http://www.regulations.gov,* including any personal information provided. To confirm receipt of your comment(s), please check *www.regulations.gov,* approximately two to three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: Ms. Heather Kitchens, telephone 571–372–6104.

SUPPLEMENTARY INFORMATION:

I. Background

The theft of intellectual property and sensitive information from all U.S. industrial sectors due to malicious cyber activity threatens economic security and national security. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Over a ten-year period, that burden would equate to an estimated $570 billion to $1.09 trillion dollars in costs. As part of multiple lines of effort focused on the security and resiliency of the Defense Industrial Base (DIB) sector, the Department is working with industry to enhance the protection of unclassified information within the supply chain. Toward this end, DoD has developed the following assessment methodology and framework to assess contractor implementation of cybersecurity requirements, both of which are being implemented by this rule: the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 DoD Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC) Framework. The NIST SP 800–171 DoD Assessment and CMMC assessments will not duplicate efforts from each assessment, or any other DoD assessment, except for rare circumstances when a re-assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance.

A. NIST SP 800–171 DoD Assessment Methodology

DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is included in all solicitations and contracts, including those using Federal Acquisition Regulation (FAR) part 12 commercial item procedures, except for acquisitions solely for commercially available off-the-shelf (COTS) items. The clause requires contractors to apply the security requirements of NIST SP 800–171 to "covered contractor information systems," as defined in the clause, that are not part of an IT service or system operated on behalf of the Government. The NIST SP 800–171 DoD Assessment Methodology provides for the assessment of a contractor's implementation of NIST SP 800-171 security requirements, as required by DFARS clause 252.204–7012. More information on the NIST SP 800–171 DoD Assessment Methodology is available at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

The Assessment uses a standard scoring methodology, which reflects the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor, and three assessment levels (Basic, Medium, and High), which reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment. A Basic Assessment is a self-assessment completed by the contractor, while Medium or High Assessments are completed by the Government. The Assessments are completed for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order.

The results of Assessments are documented in the Supplier Performance Risk System (SPRS) at *https://www.sprs.csd.disa.mil/* to provide DoD Components with visibility into the scores of Assessments already completed; and verify that an offeror has a current (*i.e.,* not more than three years old, unless a lesser time is specified in the solicitation) Assessment, at any level, on record prior to contract award.

B. Cybersecurity Maturity Model Certification Framework

Building upon the NIST SP 800–171 DoD Assessment Methodology, the CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB contractor can adequately protect sensitive unclassified information such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

The CMMC model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community. The CMMC levels and the associated sets of processes and practices are cumulative. The CMMC model encompasses the basic safeguarding requirements for FCI specified in FAR clause 52.204–21, Basic Safeguarding of Covered

Contractor Information Systems, and the security requirements for CUI specified in NIST SP 800–171 per DFARS clause 252.204–7012. Furthermore, the CMMC model includes an additional five processes and 61 practices across Levels 2–5 that demonstrate a progression of cybersecurity maturity.

Level	Description
1	Consists of the 15 basic safeguarding requirements from FAR clause 52.204–21.
2	Consists of 65 security requirements from NIST SP 800–171 implemented via DFARS clause 252.204–7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3.
3	Consists of all 110 security requirements from NIST SP 800–171, 20 CMMC practices, and 3 CMMC processes.
4	Consists of all 110 security requirements from NIST SP 800–171, 46 CMMC practices, and 4 CMMC processes.
5	Consists of all 110 security requirements from NIST SP 800–171, 61 CMMC practices, and 5 CMMC processes.

In order to achieve a specific CMMC level, a DIB company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level. CMMC assessments will be conducted by accredited CMMC Third Party Assessment Organizations (C3PAOs). Upon completion of a CMMC assessment, a company is awarded a certification by an independent CMMC Accreditation Body (AB) at the appropriate CMMC level (as described in the CMMC model). The certification level is documented in SPRS to enable the verification of an offeror's certification level and currency (*i.e.* not more than three years old) prior to contract award. Additional information on CMMC and a copy of the CMMC model can be found at *https://www.acq.osd.mil/cmmc/index.html.*

DoD is implementing a phased rollout of CMMC. Until September 30, 2025, the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, is prescribed for use in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, excluding acquisitions exclusively for COTS items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement the phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment.

CMMC will apply to all DoD solicitations and contracts, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, starting on or after October 1, 2025. Contracting officers will not make award, or exercise an option on a contract, if the offeror or contractor does not have current (*i.e.* not older than three years) certification for the required CMMC level. Furthermore, CMMC certification requirements are required to be flowed down to subcontractors at all tiers, based on the sensitivity of the unclassified information flowed down to each subcontractor.

II. Discussion and Analysis

A. NIST SP 800–171 DoD Assessment Methodology

This rule amends DFARS subpart 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting, to implement the NIST SP 800–171 DoD Assessment Methodology. The new coverage in the subpart directs contracting officers to verify in SPRS that an offeror has a current NIST SP 800–171 DoD Assessment on record, prior to contract award, if the offeror is required to implement NIST SP 800–171 pursuant to DFARS clause 252.204–7012. The contracting officer is also directed to include a new DFARS provision 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements, and a new DFARS clause 252.204–7020, NIST SP 800–171 DoD Assessment Requirements, in solicitations and contracts including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of COTS items.

The new DFARS provision 252.204–7019 advises offerors required to implement the NIST SP 800–171 standards of the requirement to have a current (not older than three years) NIST SP 800–171 DoD Assessment on record in order to be considered for award. The provision requires offerors to ensure the results of any applicable current Assessments are posted in SPRS and provides offerors with additional information on conducting and submitting an Assessment when a current one is not posted in SPRS.

The new DFARS clause 252.204–7020 requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level Assessment. The clause also requires the contractor to ensure that applicable subcontractors also have the results of a current Assessment posted in SPRS prior to awarding a subcontract or other contractual instruments. The clause also provides additional information on how a subcontractor can conduct and submit an Assessment when one is not posted in SPRS, and requires the contractor to include the requirements of the clause in all applicable subcontracts or other contractual instruments.

B. Cybersecurity Maturity Model Certification

This rule adds a new DFARS subpart, Subpart 204.75, Cybersecurity Maturity Model Certification (CMMC), to specify the policy and procedures for awarding a contract, or exercising an option on a contract, that includes the requirement for a CMMC certification. Specifically, this subpart directs contracting officers to verify in SPRS that the apparently successful offeror's or contractor's CMMC certification is current and meets the required level prior to making the award.

A new DFARS clause 252.204–7021, Cybersecurity Maturity Model Certification Requirements, is prescribed for use in all solicitations and contracts or task orders or delivery orders, excluding those exclusively for the acquisition of COTS items. This DFARS clause requires a contractor to: Maintain the requisite CMMC level for the duration of the contract; ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments; and include the requirements of the clause in all subcontracts or other contractual instruments.

The Department took into consideration the timing of the requirement to achieve a CMMC level certification in the development of this rule, weighing the benefits and risks associated with requiring CMMC level certification: (1) At time of proposal or offer submission; (2) at time of award;

or (3) after contract award. The Department ultimately adopted alternative 2 to require certification at the time of award. The drawback of alternative 1 (at time of proposal or offer submission) is the increased risk for contractors since they may not have sufficient time to achieve the required CMMC certification after the release of the Request for Information (RFI). The drawback of alternative 3 (after contract award) is the increased risk to the Department with respect to the schedule and uncertainty with respect to the case where the contractor is unable to achieve the required CMMC level in a reasonable amount of time given their current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI. The Department seeks public comment on the timing of contract award, to include the effect of requiring certification at time of award on small businesses.

C. Conforming Changes

This rule also amends the following DFARS sections to make conforming changes:

- Amends the list in DFARS section 212.301 of solicitation provisions and contract clauses that are applicable for the acquisition of commercial items to include the provisions and clauses included in this rule.
- Amends DFARS 217.207, Exercise of Options, to advise contracting officers that an option may only be exercised after verifying the contractor's CMMC level, when CMMC is required in the contract.

III. Applicability to Contracts at or Below the Simplified Acquisition Threshold and for Commercial Items, Including Commercially Available Off-the-Shelf Items

This rule creates the following new solicitation provision and contract clauses:

- DFARS 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements;
- DFARS clause 252.204–7020, NIST SP 800–171 DoD Assessment Requirements; and
- DFARS clause 252.204–7021, Cybersecurity Maturity Model Certification Requirements.

The objective of this rule is provide the Department with: (1) The ability to assess contractor implementation of NIST SP 800–171 security requirements, as required by DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting; and (2) assurances that DIB contractors can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information flowed down to subcontractors in a multi-tier supply chain. Flowdown of the requirements is necessary to respond to threats that reach even the lowest tiers in the supply chain. Therefore, to achieve the desired policy outcome, DoD intends to apply the new provision and clauses to contracts and subcontracts for the acquisition of commercial items and to acquisitions valued at or below the simplified acquisition threshold, but greater than the micro-purchase threshold. The provision and clauses will not be applicable to contracts or subcontracts exclusively for the acquisition of commercially available off-the-shelf items.

IV. Expected Cost Impact and Benefits

A. Benefits

The theft of intellectual property and sensitive information from all U.S. industrial sectors due to malicious cyber activity threatens U.S. economic and national security. The aggregate loss of intellectual property and certain unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation, as well as significantly increase risk to national security. This rule is expected to enhance the protection of FCI and CUI within the DIB sector.

B. Costs

A Regulatory Impact Analysis (RIA) that includes a detailed discussion and explanation about the assumptions and methodology used to estimate the cost of this regulatory action is available at *www.regulations.gov* (search for "DFARS Case 2019–D041" click "Open Docket," and view "Supporting Documents"). The total estimated public and Government costs (in millions) associated with this rule, calculated in perpetuity in 2016 dollars at a 7 percent discount rate, is provided as follows:

Total cost (in millions)	Public	Govt	Total
Annualized Costs	$6,500.5	$0.3	$6,500.7
Present Value Costs	92,863.6	3.7	92,867.3

The following is a breakdown of the public and Government costs and savings associated with each component of the rule:

1. NIST SP 800–171 DoD Assessments

The following is a summary of the estimated public and Government costs (in millions) associated with the NIST SP DoD Assessments, calculated in perpetuity in 2016 dollars at a 7 percent discount rate:

DoD assessments	Public	Government	Total
Annualized Costs	$6.7	$9.5	$16.3
Present Value Costs	96.1	136.2	232.3

2. CMMC Requirements

The following is a summary of the estimated public and Government costs (in millions) associated with the CMMC requirements, calculated in perpetuity in 2016 dollars at a 7 percent discount rate:

CMMC requirements	Public	Government	Total
Annualized Costs	$6,525.0	$8.9	$6,533.9
Present Value Costs	93,213.6	127.3	93,340.9

3. Elimination of Duplicate Assessments

The following is a summary of the estimated public and Government savings (in millions) associated with the elimination of duplicate assessments, calculated in perpetuity in 2016 dollars at a 7 percent discount rate:

Eliminate duplication	Public	Government	Total
Annualized Savings	-$31.2	-$18.2	-$49.4
Present Value Savings	-446.1	-259.8	-705.9

V. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is an economically significant regulatory action and, therefore, was subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is a major rule under 5 U.S.C. 804.

VI. Executive Order 13771

The rule is not subject to the requirements if E.O. 13771, because this rule is being issued with respect to a national security function of the United States.

VII. Regulatory Flexibility Act

DoD expects this rule to have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.* Therefore, an initial regulatory flexibility analysis has been performed and is summarized as follows:

A. Reasons for the Action

This rule is necessary to address threats to the U.S. economy and national security from ongoing malicious cyber activities, which includes the theft of hundreds of billions of dollars of U.S. intellectual property. Currently, the FAR and DFARS prescribe contract clauses intended to protect FCI and CUI within the DoD supply chain. Specifically, the clause at FAR 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, is prescribed at FAR 4.1903 for use in Government solicitations and contracts and requires contractors and subcontractors to apply basic safeguarding requirements when processing, storing, or transmitting FCI in or from covered contractor information systems. The clause focuses on ensuring a basic level of cybersecurity hygiene and is reflective of actions that a prudent business person would employ.

In addition, DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires defense contractors and subcontractors to provide "adequate security" to store, process, or transmit CUI on information systems or networks, and to report cyber incidents that affect these systems or networks. The clause states that to provide adequate security, the Contractor shall implement, at a minimum, the security requirements in "National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations." Contractors are also required to flow down DFARS Clause 252.204–7012 to all subcontracts, which involve CUI.

However, neither the FAR clause, nor the DFARS clause, provide for DoD verification of a contractor's implementation of basic safeguarding requirements or the security requirements specified in NIST SP 800–171 prior to contract award.

Under DFARS clause 252.204–7012, DIB companies self-attest that they will implement the requirements in NIST SP 800–171 upon submission of their offer. A contractor can document implementation of the security requirements in NIST SP 800–171 by having a system security plan in place to describe how the security requirements are implemented, in addition to associated plans of action to describe how and when any unimplemented security requirements will be met. As a result, the current regulation enables contractors and subcontractors to process, store, or transmit CUI without having implemented all of the 110 security requirements and without establishing enforceable timelines for addressing shortfalls and gaps.

Findings from DoD Inspector General report (DODIG–2019–105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information. The report emphasizes that malicious actors can exploit the vulnerabilities of contractors' networks and systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies.

Although DoD contractors must include DFARS clause 252.204–7012 in subcontracts for which subcontract performance will involve covered defense information (DoD CUI), this does not provide the Department with sufficient insights with respect to the cybersecurity posture of DIB companies throughout the multi-tier supply chain for any given program or technology development effort.

Furthermore, given the size and scale of the DIB sector, the Department cannot scale its organic cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors every three years. As a result, the Department's organic assessment capability is best suited for conducting targeted assessments for a subset of DoD contractors.

Finally, the current security requirements specified in NIST SP 800–171 per DFARS clause 252.204–7012, do not sufficiently address additional threats to include Advanced Persistent Threats (APTs).

Because of these issues and shortcomings and the associated risks to national security, the Department determined that the status quo was not acceptable and developed a two-pronged approach to assess and verify the DIB's ability to protect the FCI and CUI on its information systems or networks, which is being implemented by this rule:

- *The National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 DoD Assessment Methodology.* A standard methodology to assess contractor implementation of the cybersecurity requirements in NIST SP 800–171,

"Protecting Controlled Unclassified Information (CUI) In Nonfederal Systems and Organizations."

• *The Cybersecurity Maturity Model Certification (CMMC) Framework.* A DoD certification process that measures a company's institutionalization of processes and implementation of cybersecurity practices.

B. Objectives of, and Legal Basis for, the Rule

This rule establishes a requirement for contractors to have a current NIST SP 800–171 DoD Assessment and the appropriate CMMC level certification prior to contract award and during contract performance. The objective of the rule is to provide the Department with: (1) The ability to assess at a corporate-level a contractor's implementation of NIST SP 800–171 security requirements, as required by DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting; and (2) assurances that a DIB contractor can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

1. NIST SP 800–171 DoD Assessment Methodology

In February 2019, the Under Secretary of Defense for Acquisition and Sustainment directed the Defense Contract Management Agency (DCMA) to develop a standard methodology to assess contractor implementation of the cybersecurity requirements in NIST SP 800–171 at the corporate or entity level. The DCMA Defense Industrial Base Cybersecurity Assessment Center's NIST SP 800–171 DoD Assessment Methodology is the Department's initial strategic DoD/corporate-wide assessment of contractor implementation of the mandatory cybersecurity requirements established in the contracting regulations. Results of a NIST SP 800–171 DoD Assessment reflect the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor, and may be conducted at one of three assessment levels. The DoD Assessment Methodology provides the following benefits:

• *Enables Strategic Assessments at the Entity-level.* The NIST SP 800–171 DoD Assessment Methodology enables DoD to strategically assess a contractor's implementation of NIST SP 800–171 on existing contracts that include DFARS clause 252.204–7012, and to provide an objective assessment of a contractor's NIST SP 800–171 implementation status.

• *Reduces Duplicative or Repetitive Assessments of our Industry Partners.* Assessment results will be posted in the Supplier Performance Risk System (SPRS), DoD's authoritative source for supplier and product performance information. This will provide DoD Components with visibility to summary level scores, rather than addressing implementation of NIST SP 800–171 on a contract-by-contract approach. Conducting such assessments at a corporate- or entity-level, significantly reduces the need to conduct assessments at the program or contract level, thereby reducing the cost to both DoD and industry.

• *Provides a Standard Methodology for Contractors to Self-assess Their Implementation of NIST SP 800–171.* The Basic Assessment provides a consistent means for contractors to review their system security plans prior to and in preparation for either a DoD or CMMC assessment.

The NIST SP 800–171 DoD Assessment Methodology provides a means for the Department to assess contractor implementation of these requirements as the Department transitions to full implementation of the CMMC, and a means for companies to self-assess their implementation of the NIST SP 800–171 requirements prior to either a DoD or CMMC assessment.

2. The CMMC Framework

Section 1648 of the National Defense Authorization Act for Fiscal Year (FY) 2020 (Pub. L. 116–92) directs the Secretary of Defense to develop a risk-based cybersecurity framework for the DIB sector, such as CMMC, as the basis for a mandatory DoD standard. Building upon the NIST SP 800–171 DoD Assessment Methodology, the CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB contractor can adequately protect sensitive unclassified information (*i.e.* FCI and CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. Implementation of the CMMC Framework is intended to solve the following policy problems:

• *Verification of a contractor's cybersecurity posture.* DFARS clause 252.204–7012 does not provide for the DoD verification of a DIB contractor's implementation of the security requirements specified in NIST SP 800–171 prior to contract award. DIB companies self-attest that they will implement the requirements in NIST SP 800–171 upon submission of their offer. Findings from DoD Inspector General report (DODIG–2019–105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information. CMMC adds the element of verification of a DIB contractor's cybersecurity posture through the use of accredited C3PAOs. The company must achieve the CMMC level certification required as a condition of contract award.

• *Comprehensive implementation of cybersecurity requirements.* Under DFARS clause 252.204–7012, a contractor can document implementation of the security requirements in NIST SP 800–171 by having a system security plan in place to describe how the security requirements are implemented, in addition to associated plans of action to describe how and when any unimplemented security requirements will be met. The CMMC framework does not allow a DoD contractor or subcontractor to achieve compliance status through the use of plans of action. In general, CMMC takes a risk-based approach to addressing cyber threats. Based on the type and sensitivity of the information to be protected, a DIB company must achieve the appropriate CMMC level and demonstrate implementation of the requisite set of processes and practices. Although the security requirements in NIST SP 800–171 addresses a range of threats, additional requirements are needed to further reduce the risk of Advanced Persistent Threats (APTs). An APT is an adversary that possesses sophisticated levels of expertise and significant resources, which allow it to create opportunities to achieve its objectives by using multiple attack vectors (*e.g.* cyber, physical, and deception). The CMMC model includes additional processes and practices in Levels 4 and 5 that are focused on further reducing the risk of APT threats. The CMMC implementation will provide the Department with an ability to illuminate the supply chain, for the first time, at scale across the entire DIB sector. The CMMC framework requires contractors to flow down the appropriate CMMC

certification requirement to subcontractors throughout the entire supply chain. DIB companies that do not process, store, or transmit CUI, must obtain a CMMC level 1 certification. DIB companies that process, store, or transmit CUI must achieve a CMMC level 3 or higher, depending on the sensitivity of the information associated with a program or technology being developed.

- *Scale and Depth.* DoD contractors must include DFARS clause 252.204–7012 in subcontracts for which subcontract performance will involve covered defense information (DoD CUI), but this does not provide the Department with sufficient insights with respect to the cybersecurity posture of DIB companies throughout the multi-tier supply chain for any given program or technology development effort. Given the size and scale of the DIB sector, the Department cannot scale its organic cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors every three years. As a result, the Department's organic assessment capability is best suited for conducting targeted assessments for a subset of DoD contractors that support prioritized programs and/or technology development efforts. CMMC addresses the challenges of the Department scaling its organic assessment capability by partnering with an independent, non-profit CMMC–AB that will accredit and oversee multiple third party assessment organizations (C3PAOs) which in turn, will conduct on-site assessments of DoD contractors throughout the multi-tier supply chain. DIB companies will be able to directly schedule assessments with an accredited C3PAO for a specific CMMC level. The cost of these CMMC assessments will be driven by multiple factors including market forces, the size and complexity of the network or enclaves under assessment, and the CMMC level.
- *Reduces Duplicate or Repetitive Assessments of our Industry Partners.* Assessment results will be posted in the Supplier Performance Risk System (SPRS), DoD's authoritative source for supplier and product performance information. This will provide DoD Components with visibility to CMMC certifications for DIB contractor networks and an alternative to addressing implementation of NIST SP 800–171 on a contract-by-contract approach—significantly reducing the need to conduct assessments at the program level, thereby reducing the cost to both DoD and industry.

C. Description of and Estimate of the Number of Small Entities to Which the Rule Will Apply

This rule will impact all small businesses that do business with Department of Defense, except those competing on contracts or orders that are exclusively for COTS items or receiving contracts or orders valued at or below the micro-purchase threshold.

1. The NIST SP 800–171 DoD Assessment Methodology

According to data available in the Electronic Data Access system for fiscal years (FYs) 2016, 2017, and 2018, on an annual basis DoD awards on average 485,859 contracts and orders that contain DFARS clause 252.204–7012 to 39,204 unique awardees, of which 262,509 awards (54 percent) are made to 26,468 small entities (68 percent). While there may be some entities that have contracts that contain the clause at 252.204–7012, but never process CUI and, therefore, do not have to implement NIST SP 800–171, it is not possible for DoD to estimate what fraction of unique entities fall into this category. Assuming all of these small entities have covered contractor information systems that are required to be in compliance with NIST SP 800–171, then all of these entities would be required to have, at minimum, a Basic Assessment in order to be considered for award.

The requirement for the Basic Assessment would be imposed through incorporation of the new solicitation provision and contract clause in new contracts and orders. As such, the requirement to have completed a Basic Assessment is expected to phase-in over a three-year period, thus impacting an estimated 8,823 small entities each year. It is expected that the Medium and High Assessments, on the other hand, will be conducted on a finite number of awardees each year based on the capacity of the Government to conduct these assessments. DoD estimates that 200 unique entities will undergo a Medium Assessment each year, of which 148 are expected to be small entities. High Assessments are expected to be conducted on approximately 110 unique entities each year, of which 81 are expected to be small entities. DoD Assessments are valid for three years, so small entities will be required to renew, at minimum, their basic assessment every three years in order to continue to receive DoD awards or to continue performance on contracts and orders with options. The following is a summary of the number of small entities that will be required to undergo NIST SP 800–171 DoD Assessments over a three-year period:

Assessment	Year 1	Year 2	Year 3
Basic	8,823	8,823	8,823
Medium	148	148	148
High	81	81	81

The top five NAICS code industries expected to be impacted by this rule are as follows: 541712, Research and Development in the Physical, Engineering, and Life Sciences (Except Biotechnology); 541330, Engineering Services; 236220, Commercial and Institutional Building Construction; 541519, Other Computer Related Services; and 561210, Facilities Support Services. These NAICS codes were selected based on a review of NAICS codes associated with awards that include the clause at DFARS 252.204–7012.

2. The CMMC Framework

Given the enterprise-wide implementation of CMMC, the Department developed a five-year phased rollout strategy. The rollout is intended to minimize the financial impacts to the industrial base, especially small entities, and disruption to the existing DoD supply chain. The Office of the Secretary of Defense staff is coordinating with the Military Services and Department Agencies to identify candidate contracts during the first five years of implementation that will include the CMMC requirement in the statement of work.

Prior to October 1, 2025, this rule impacts certain large and small businesses that are competing on acquisitions that specify a requirement for CMMC in the statement of work. These businesses will be required to have the stated CMMC certification level at the time of contract award. Inclusion of a CMMC requirement in a

solicitation during this time period must be approved by the USD(A&S). It is estimated that 129,810 unique entities will pursue their initial CMMC certification during the initial five-year period. By October 1, 2025, all entities receiving DoD contracts and orders, other than contracts or orders exclusively for commercially available off-the-shelf items or those valued at or below the micro-purchase threshold, will be required to have the CMMC Level identified in the solicitation, but which at minimum will be a CMMC Level 1 certification. CMMC certifications are valid for three years; therefore, large and small businesses will be required to renew their certification every three years.

Based on information from the Federal Procurement Data System (FPDS), the number of unique prime contractors is 212,657 and the number of known unique subcontractors is 8,309. Therefore, the total number of known unique prime contractors and subcontractors is 220,966, of which approximately 163,391 (74 percent) are estimated to be unique small businesses. According to FPDS, the average number of new contracts for unique contractors is 47,905 for any given year. The timeline required to implement CMMC across the DoD contractor population will be approximately 7 years. The phased rollout plan for years 1–7 for small entities is detailed below with the total number of unique DoD contractors and subcontractors specified. The rollout assumes that for every unique prime contractor there are approximately 100 unique subcontractors. Each small business represented in the table would be required to pursue recertification every three years in order to continue to do business with DoD.

Year	Level 1	Level 2	Level 3	Level 4	Level 5	Total
1	665	110	335	0	0	1,110
2	3,323	555	1,661	2	2	5,543
3	11,086	1,848	5,543	4	4	18,485
4	21,248	3,542	10,624	6	6	35,426
5	21,245	3,541	10,623	7	7	35,423
6	21,245	3,541	10,623	7	7	35,423
7	19,180	3,197	9,590	7	7	31,981
1–7	97,992	16,334	48,999	33	33	163,391

The top five NAICS code industries expected to be impacted by this rule are as follows: 541712, Research and Development in the Physical, Engineering, and Life Sciences (Except Biotechnology); 541330, Engineering Services; 236220, Commercial and Institutional Building Construction; 541519, Other Computer Related Services; and 561210, Facilities Support Services. These NAICS codes are the same as the DoD Assessment NAICS codes and were selected based on a review of NAICS codes associated with awards that include the clause at FAR 52.204–21 or DFARS 252.204–7012.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Rule

Details on the compliance requirements and associated costs, savings, and benefits of this rule are provided in the Regulatory Impact Analysis referenced in section IV of this preamble. The following is a summary of the compliance requirements and the estimated costs for small entities to undergo a DoD NIST SP 800–171 Assessment or obtain a CMMC certification. For both the DoD Assessment Methodology and the CMMC Framework, the estimated public costs are based on the cost for an entity to pursue each type of assessment: The Basic, Medium, or High Assessment under the DoD Assessment Methodology; or the CMMC Level 1, 2, 3, 4, or 5 certifications. The estimated costs attributed to this rule do not include the costs associated with compliance with the existing cybersecurity requirements under the clause at FAR 52.204–21 or associated with implementing NIST SP 800–171 in accordance with the clause at DFARS 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Contractors who have been awarded a DoD contract that include these existing contract clauses should have already implemented these cybersecurity requirements and incurred the associated costs; therefore, those costs are not attributed to this rule.

1. DoD Assessment Methodology

To comply with NIST SP 800–171 a company must (1) implement 110 security requirements on their covered contractor information systems; or (2) document in a "system security plan" and "plans of action" those requirements that are not yet implemented and when the requirements will be implemented. All offerors that are required to implement NIST SP 800–171 on covered contractor information systems pursuant to DFARS clause 252.204–7012, will be required to complete a Basic Assessment and upload the resulting score to the Supplier Risk Management System (SPRS), DoD's authoritative source for supplier and product performance information. The Basic Assessment is a self-assessment done by the contractor using a specific scoring methodology that tells the Department how many security requirements have not yet been implemented and is valid for three years. A company that has fully implemented all 110 NIST SP 800–171 security requirements, would have a score of 110 to report in SPRS for their Basic Assessment. A company that has unimplemented requirements will use the scoring methodology to assign a value to each unimplemented requirement, add up those values, and subcontract the total value from 110 to determine their score.

In accordance with NIST SP 800–171, a contractor should already be aware of the security requirements they have not yet implemented and have documented plans of action for those requirements; therefore, the burden associated with conducting a self-assessment is the time burden associated with calculating the score. DoD estimates that the burden to calculate the Basic Assessment score is thirty minutes per entity at a journeyman-level-2 rate of pay (0.50 hour * $99.08/hour = $49.54/assessment)).

To submit the Basic Assessment, the contractor is required to complete 6 fields: System security plan name (if more than one system is involved); CAGE code associated with the plan; a brief description of the plan architecture; date of the assessment; total score; and the date a score of 110 will be achieved. All of this data is available from the Basic Assessment itself, the existing system security plan, and the plans of action. The contractor selects the date when the last plan of

action will be complete as the date when a score of 110 will be achieved. The burden to submit a Basic Assessment for posting in SPRS is estimated to be 15 minutes per entity at a journeyman-level-2 rate of pay (0.25 hour * $99.08/hour = $24.77/assessment)). Therefore, the total cost per assessment per entity is approximately $74.31 ($49.54 + $24.77).

The estimate for the rate of pay for both preparation and submission of the Basic Assessment is journeyman-level-2, which is an employee who has the equivalent skills, responsibilities, and experience as a General Schedule (GS) 13 Federal Government employee. While these are rather simple tasks that can reasonably be completed by a GS–11 equivalent employee, or even a GS–9 clerk, the GS–13 (or perhaps GS–11) is the most likely grade for several reasons. First, in a small company, the number of IT personnel are very limited. The employee that is available to complete this task would also have significant responsibilities for operation and maintenance of the IT system and, therefore, be at a higher grade than would otherwise be required if the only job was to prepare and submit the assessment. Second, while the calculation of the assessment is simple, the personnel who would typically have access to and understand the system security plan and plans of action in order to complete the Basic Assessment would be at the higher grade. Third, while the actual submission is a simple task, the person who would complete the assessment and submit the data in SPRS would be the person with SPRS access/responsibilities, and therefore at the higher grade. Fourth, given that proper calculation of the score and its submission may well determine whether or not the company is awarded the contract, the persons preparing and submitting the report are likely to be at a higher grade than is actually required to ensure this is done properly.

After a contract is awarded, DoD may choose to conduct a Medium or High Assessment of an offer based on the criticality of the program or the sensitivity of information being handled by the contractor. Under both the Medium and High Assessment DoD assessors will be reviewing the contractor's system security plan description of how each NIST SP 800–171 requirement is met and will identify any descriptions that may not properly address the security requirements. The contractor provides DoD access to its facilities and personnel, if necessary, and prepares for/participates in the assessment conducted by the DoD. Under a High Assessment a contractor will be asked to demonstrate their system security plan. DoD will post the results in SPRS.

For the Medium Assessment, DoD estimates that the burden for a small entity to make the system security plan and supporting documentation available for review by the DoD assessor is one hour per entity at a journeyman-level-2 rate of pay, a cost of $99.08/assessment (1 hour * $99.08/hour). It is estimated that the burden for a small entity to participate in the review and discussion of the system security plan and supporting documents with the DoD assessor is three hours, with one journeyman-level-2 and one senior-level-2 contractor employee participating in the assessment, a cost of $710.40/assessment ((3 hours * $99.08/hour = $297.24) + (3 hours * $137.72/hour = $413.16)). Assuming issues are identified by the DoD Assessor, DoD estimates that the burden for a small entity to determine and provide to DoD the date by which the issues will be resolved is one hour per entity at a journeyman-level rate of pay, a cost of $99.08/assessment (1 hour * $99.08/hour). Therefore, total estimated cost for a small entity that undergoes a Medium Assessment is $908.56/assessment ($99.08 + $710.40 + $99.08).

For the High Assessment, DoD estimates that the burden for a small entity to participate in the review and discussion of the system security plan and supporting documents to the DoD assessors is 116 hours per entity at a cost of $14,542.24/assessment. The cost estimate is based on 2 senior-level-2 employees dedicating 32 hours each, 8 senior-level-1 employees dedicating 4 hours each, and 10 journeyman-level employees dedicating 2 hours each ((2 * 32 hours * $137.72/hour = $8,814.08) + (8 * 4 hours * 117.08/hour = $3,746.56) + (10 * 2 hours * $99.08/hour = 1,981.60)). It is estimated that the burden to make the system security plan and supporting documentation available for review by the DoD assessors, prepare for demonstration of requirements implementation, and to conduct post review activities is 304 hours per entity, at a cost of $36,133.76/assessment. The cost estimate is based on 2 senior-level-2 employees dedicating 48 hours each, 8 senior-level-1 employees dedicating 16 hours each, and 10 journeyman-level employees dedicating 8 hours each ((2 * 48 hours * $137.72/hour = $13,221.12) + (8 * 16 hours * 117.08/hour = $14,986.24) + (10 * 8 hours * $99.08/hour = $7,926.40)). Therefore, total estimated cost for a small entity that undergoes a High Assessment is $50,676/assessment ($14,542.24 + $36,133.76). DoD considers this to be the upper estimate of the cost, as it assumes a very robust information technology workforce. For many smaller companies, which may not have a complex information system to manage, the information system staff will be a much more limited, and labor that can be devoted (or is necessary) to prepare for and participate in the assessment is likely to be significantly less than estimated.

The following table provides the estimated annual costs for small entities to comply with the DoD Assessment requirements of this rule. Since assessments are valid for three years, the cost per assessment has been divided by three to estimate the annual cost per entity:

Assessment	Cost/assessment	Annual cost/entity	Total unique entities	Annual cost all entities
Basic	$75	$25	26,469	$655,637
Medium	909	303	444	134,467
High	50,676	16,892	243	4,104,756
Total			27,156	4,894,860

The following table presents the average annual cost per small entity for each DoD Assessment as a percentage of the annual revenue for a small entity for four of the top five NAICS codes. The low-end of the range of annual revenues presented in the table includes the average annual revenue for smaller sized firms. The high-end of the range includes the maximum annual revenue allowed by the Small Business Administration (SBA) for a small

business, per the SBA's small business size standards published at 13 CFR 121.201. NAICS code 541712 is excluded, because it is no longer an active NAICS code and the prior size standard was based on number of employees.

NAICS code	Range of annual revenues for small businesses (in millions)	Basic assessment annual cost as % of annual revenue	Medium assessment annual cost as % of annual revenue	High assessment annual cost as % of annual revenue
541330	$5–16.5	0.0005–0.0002	0.0061–0.0018	0.3378–0.1024
236220	$10–$39.5	0.0002–0.0001	0.0030–0.0008	0.1689–0.0428
541519	$10–$30.0	0.0002–0.0001	0.0030–0.0010	0.1689–0.0563
561210	$10–$41.5	0.0002–0.0001	0.0030–0.0007	0.1689–0.0407

2. CMMC Framework

This rule adds DFARS clause 252.204–7021, Cybersecurity Maturity Model Certification Requirement, which requires the contractor to have the CMMC certification at the level required in the solicitation by contract award and maintain the required CMMC level for the duration of the contract. In order to achieve a specific CMMC level, a DIB company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

The following table provides a high-level description of the processes and practices evaluated during a CMMC assessment at each level; however, more specific information on the processes and practices associated with each CMMC Level is available at *https://www.acq.osd.mil/cmmc/index.html.*

Level	Description
1	Consists of the 15 basic safeguarding requirements from FAR clause 52.204–21.
2	Consists of 65 security requirements from NIST SP 800–171 implemented via DFARS clause 252.204–7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3.
3	Consists of all 110 security requirements from NIST SP 800–171, 20 CMMC practices, and 3 CMMC processes.
4	Consists of all 110 security requirements from NIST SP 800–171, 46 CMMC practices, and 4 CMMC processes.
5	Consists of all 110 security requirements from NIST SP 800–171, 61 CMMC practices, and 5 CMMC processes.

CMMC Assessments will be conducted by C3PAOs, which are accredited by the CMMC–AB. C3PAOs will provide CMMC Assessment reports to the CMMC–AB who will then maintain and store these reports in appropriate database(s). The CMMC–AB will issue CMMC certificates upon the resolution of any disputes or anomalies during the conduct of the assessment. These CMMC certificates will be distributed to the DIB contractor and the requisite information will be posted in SPRS.

If a contractor disputes the outcome of a C3PAO assessment, the contractor may submit a dispute adjudication request to the CMMC–AB along with supporting information related to claimed errors, malfeasance, or ethical lapses by the C3PAO. The CMMC–AB will follow a formal process to review the adjudication request and provide a preliminary evaluation to the contractor and C3PAO. If the contractor does not accept the CMMC–AB preliminary finding, the contractor may request an additional assessment by the CMMC–AB staff.

The costs associated with the preparation and the conduct of CMMC Assessments assumes that a small DIB company, in general, possesses a less complex and less expansive IT and cybersecurity infrastructure and operations relative to a larger DIB company. In estimating the cost for a small DIB company to obtain a CMMC certification, DoD took into account non-recurring engineering costs, recurring engineering costs, the cost to participate in the assessment, and re-certification costs:

- Nonrecurring engineering costs consist of hardware, software, and the associated labor. The costs are incurred only in the year of the initial assessment.
- Recurring engineering costs consist of any recurring fees and associated labor for technology refresh. The recurring engineering costs associated with technology refresh have been spread uniformly over a 5-year period (*i.e.*, 20% each year as recurring engineering costs).
- Assessment costs consist of contractor support for pre-assessment preparations, the actual assessment, and any post-assessment work. These costs also include an estimate of the potential C3PAO costs for conducting CMMC Assessment, which are comprised of labor for supporting pre-assessment preparations, actual assessment, and post-assessment work, plus travel cost.
- Re-certification costs are the same as the initial certification cost.

The following is a summary of the estimated costs for a small entity to achieve certification at each CMMC Level.

i. Level 1 Certification

Contractors pursuing a Level 1 Certification should have already implemented the 15 existing basic safeguarding requirements under FAR clause 52.204–21. Therefore, there are no estimated nonrecurring or recurring engineering costs associated with CMMC Level 1.

DoD estimates that the cost for a small entity to support a CMMC Level 1 Assessment or recertification is $2,999.56:

- *Contractor Support.* It is estimated that one journeyman-level-1 employee will dedicate 14 hours to support the assessment (8 hours for pre- and post-assessment support + 6 hours for the assessment). The estimated cost is $1,166.48 (1 journeyman * $83.32/hour * 14 hours).
- *C3PAO Assessment.* It is estimated that one journeyman-level-1 employee will dedicate 19 hours to conduct the assessment (8 hours for pre- and post-assessment support + 6 hours for the assessment + 5 hours for travel). Each employee is estimated to have 1 day of per diem for travel. The estimated cost

is $1,833.08 ((1 journeyman * $83.32/hour * 19 hours = $1,583.08) + (1 employees * 1 day * $250/day = $250 travel costs)).

ii. Level 2 Certification

Contractors pursuing a Level 2 Certification should have already implemented the 65 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation of 9 new requirements (7 CMMC practices and 2 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $8,135. The estimated recurring engineering cost per entity per year is $20,154.

DoD estimates that the cost for a small entity to support a CMMC Level 2 Assessment or recertification is $22,466.88.

- *Contractor Support.* It is estimated that two senior-level-1 employees will dedicate 48 hours each to support the assessment (24 hours for pre- and post-assessment support + 24 hours for the assessment). The estimated cost is $11,239.68 (2 senior * $117.08/hour * 48 hours).
- *C3PAO Assessment.* It is estimated that one journeyman-level-2 employee and one senior-level-1 employee will dedicate 45 hours each to conduct the assessment (16 hours for pre- and post-assessment support + 24 hours for the assessment + 5 hours for travel). Each employee is estimated to have 3 days of per diem for travel. The estimated cost is $11,227.20 ((1 senior * $117.08/hour * 45 hours = $5,268.60) + (1 journeyman * $99.08/hour * 45 hours = $4,458.60) + (2 employees * 3 days * $250/day = $1,500 travel costs)).

iii. Level 3 Certification

Contractors pursuing a Level 3 Certification should have already implemented the 110 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation 23 new requirements (20 CMMC practices and 3 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $26,214. The estimated recurring engineering cost per entity per year is $41,666.

DoD estimates that the cost for a small entity to support a CMMC Level 3 assessment or recertification is $51,095.60.

- *Contractor Support.* It is estimated that three senior-level-1 employees will dedicate 64 hours each to support the assessment (32 hours for pre- and post-assessment support + 32 hours for the assessment). The estimated cost is $22,479.36 (3 seniors * $117.08/hour * 64 hours).
- *C3PAO Assessment.* It is estimated that one senior-level-1 employee and three journeyman-level-2 employees will dedicate 57 hours each to conduct the assessment (24 hours for pre- and post-assessment support + 32 hours for the assessment + 5 hours for travel). Each employee is estimated to have 5 days of per diem for travel. The estimated cost is $28,616.24 ((1 senior * $117.08/hour * 57 hours = $6,673.56) + (3 journeyman * $99.08/hour * 57 hours = $16,942.68) + (4 employees * 5 days * $250/day = $5,000 travel costs)).

iv. Level 4 Certification

Contractors pursuing a Level 4 Certification should have already implemented the 110 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation 50 new requirements (46 CMMC practices and 4 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $938,336. The estimated recurring engineering cost per entity per year is $301,514.

DoD estimates that the cost for a small entity to support a CMMC Level 4 Assessment or recertification is $70,065.04.

- *Contractor Support.* It is estimated that three senior-level-2 employees will dedicate 80 hours each to support the assessment (40 hours for pre- and post-assessment support + 40 hours for the assessment). The estimated cost is $33,052.80 (3 seniors * $137.72/hour * 80 hours)
- *C3PAO Assessment.* It is estimated that one senior-level-2 employee and three journeyman-level-2 employees will dedicate 69 hours each to conduct the assessment (32 hours for pre- and post-assessment support + 48 hours for the assessment + 5 hours for travel). Each employee is estimated to have 5 days of per diem for travel, plus airfare. The estimated cost is $37,012.24 ((1 senior * $137.72/hour * 69 hours = $9502.68) + (3 journeyman * $99.08/hour * 69 hours = $20,509.56) + (4 employees * 5 days * $250/day = $5,000 travel costs) + (4 employees * $500 = $2,000 airfare)).

v. Level 5 Certification

Contractors pursuing a Level 5 Certification should have already implemented the 110 existing NIST SP 800–171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation 66 new requirements (61 CMMC practices and 5 CMMC processes). The estimated nonrecurring engineering cost per entity per assessment/recertification is $1,230,214. The estimated recurring engineering cost per entity per year is $384,666.

DoD estimates that the cost for a small entity to support a CMMC Level 5 Assessment or recertification is $110,090.80.

- *Contractor Support.* It is estimated that four senior-level-2 employees will dedicate 104 hours each to support the assessment (48 hours for pre- and post-assessment support + 56 hours for the assessment). The estimated cost is $57,291.52 (4 senior * $137.72/hour * 104 hours).
- *C3PAO Assessment.* It is estimated that one senior-level-2 employee, two senior-level-1 employees, and one journeyman-level-2 employee will dedicate 93 hours each to conduct the assessment (32 hours for pre- and post-assessment support + 56 hours for the assessment + 5 hours for travel). Each employee is estimated to have 7 days of per diem for travel. The estimated cost is $52,799.28 ((1 senior * $137.72/hour * 93 hours = $12,807.96) + (2 senior * $117.08/hour * 93 hours = $21,776.88) + (1 journeyman * $99.08/hour * 93 hours = $9,214.44) + (4 employees * 7 days * $250/day = $7,000 travel costs) + (4 employees * $500 = $2,000 airfare)).

vi. Total Estimated Annual Costs

The following table provides a summary of the total estimated annual costs for an individual small entity to obtain each CMMC certification level. Nonrecurring engineering costs are spread over a 20-year period to determine the average annual cost per entity. Assessment costs have been spread over a 3-year period, since entities will participate in a reassessment every 3 years.

CMMC cert	Average nonrecurring engineering costs	Recurring engineering costs	Average assessment costs	Total annual assessment cost
Level 1	$0	$0	$1,000	$1,000

CMMC cert	Average nonrecurring engineering costs	Recurring engineering costs	Average assessment costs	Total annual assessment cost
Level 2	407	20,154	7,489	28,050
Level 3	1,311	41,666	17,032	60,009
Level 4	46,917	301,514	23,355	371,786
Level 5	61,511	384,666	36,697	482,874

The following table presents the average annual cost per small entity for CMMC certifications at levels 1 through 3 as a percentage of the annual revenue for a small entity for four of the top five NAICS codes. The low-end of the range of annual revenues presented in the table includes the average annual revenue for smaller sized firms. The high-end of the range includes the maximum annual revenue allowed by the SBA for a small business, per the SBA's small business size standards published at 13 CFR 121.201. NAICS code 541712 is excluded, because it is no longer an active NAICS code and the prior size standard was based on number of employees.

NAICS code	Range of annual revenues for small businesses (in millions)	CMMC level 1 annual cost as % of annual revenue	CMMC level 2 annual cost as % of annual revenue	CMMC level 3 annual cost as % of annual revenue
541330	$5–$16.5	0.0200–0.0061	0.5610–0.1700	1.2002–0.3637
236220	$10–$39.5	0.0100–0.0025	0.2805–0.0710	0.6001–0.1519
541519	$10–$30.0	0.0100–0.0033	0.2805–0.0935	0.6001–0.2000
561210	$10–$41.5	0.0100–0.0024	0.2805–0.0676	0.6001–0.1446

For CMMC certification at levels 4 and 5, the following table presents the annual cost per small entity for CMMC certification at levels 4 and 5 as a percentage of the low, average, and high annual revenues for entities that have represented themselves as small in the System for Award Management (SAM) for their primary NAICS code and are performing on contracts that could be subject to a CMMC level 4 or 5 certification requirements. The values of the low, average, and high annual revenues are based on an average of the annual receipt reported in SAM by such entities for FY16 through FY20.

FY16 thru FY20	Annual revenue of entities represented as small for primary NAICS	Level 4 certification cost as % of annual revenue	Level 5 certification cost as % of annual revenue
Low	$6.5 million	5.67	7.36
Average	$22.9 million	1.62	2.11
High	$85 million	0.43	0.56

The following is a summary of the estimated annual costs in millions for all 163,391 small entities to achieve their initial CMMC certifications (and recertifications every three years) over a 10-year period:

Year	Level 1	Level 2	Level 3	Level 4	Level 5
1	$1.99	$5.58	$39.86	$0.00	$0.00
2	9.97	30.39	211.58	2.62	3.45
3	33.25	107.20	742.65	5.84	7.67
4	65.73	232.90	1,595.23	9.67	12.66
5	73.69	314.23	2,105.53	12.93	16.91
6	96.98	414.64	2,746.50	15.18	19.82
7	123.26	509.08	3,342.95	17.43	22.74
8	73.69	421.22	2,669.25	10.58	13.68
9	96.98	450.27	2,867.60	10.72	13.90
10	123.26	483.07	3,091.56	10.86	14.13

E. Relevant Federal Rules, Which May Duplicate, Overlap, or Conflict With the Rule

The rule does not duplicate, overlap, or conflict with any other Federal rules. Rather this rule validates and verifies contractor compliance with the existing cybersecurity requirements in FAR clause 52.204–21 and DFARS clause 252.204–7012, and ensures that the entire DIB sector has the appropriate cybersecurity processes and practices in place to properly protect FCI and CUI during performance of DoD contracts.

F. Description of Any Significant Alternatives to the Rule Which Accomplish the Stated Objectives of Applicable Statutes and Which Minimize Any Significant Economic Impact of the Rule on Small Entities

DoD considered and adopted several alternatives during the development of

this rule that reduce the burden on small entities and still meet the objectives of the rule. These alternatives include: (1) Exempting contracts and orders exclusively for the acquisition of commercially available off-the-shelf items; and (2) implementing a phased rollout for the CMMC portion of the rule and stipulating that the inclusion a CMMC requirement in new contracts until that time be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment. Additional alternatives were considered, however, it was determined that these other alternatives did not achieve the intended policy outcome.

1. CMMC Model and Implementation

The Regulatory Impact Analysis (RIA) referenced in section IV of this preamble estimates that the total number of unique DoD contractors and subcontractors is 220,966, with approximately 163,391 or 74% being small entities. The RIA also specifies the estimates for the percentage of all contractors and subcontractors associated with each CMMC level. These estimates indicate that the vast majority of small entities (*i.e.,* 163,325 of 163,391 or 99.96%) will be required to achieve CMMC Level 1–3 certificates during the initial rollout. The Department looked at Levels 1 through 5 to determine if there were alternatives and whether these alternatives met the intended policy outcome.

For CMMC Level 1, the practices map directly to the basic safeguarding requirements specified in the clause at FAR 52.204–21. The phased rollout estimates that the majority of small entities (*i.e.,* 97,992 of the 163,325 or 60%) will be required to achieve CMMC Level 1. The planned implementation of CMMC Level 1 adds a verification component to the existing FAR clause by including an on-site assessment by a credentialed assessor from an accredited C3PAO. The on-site assessment verifies the implementation of the required cybersecurity practices and further supports the physical identification of contractors and subcontractors in the DoD supply chain. In the aggregate, the estimated cost associated with supporting this on-site assessment and approximated C3PAO fees does not represent a cost-driver with respect to CMMC costs to small entities across levels. An alternative to an on-site assessment is for contractors to provide documentation and supporting evidence of the proper implementation of the required cybersecurity practices through a secure online portal. These artifacts would then be reviewed and checked virtually by an accredited assessor prior to the CMMC–AB issuing a CMMC Level 1 certificate. The drawback of this alternative is the inability of the contractor to interact with the C3PAO assessor in person and provide evidence directly without transmitting proprietary information. Small entities will not receive as much meaningful and interactive feedback that would be part of a Level 1 on-site assessment.

For CMMC Level 2, the practices encompass only 48 of the 110 security requirements of NIST SP 800–171, as specified in DFARS clause 252.204–7012, and 7 additional cybersecurity requirements. In addition, CMMC Level 2 includes two process maturity requirements. The phased rollout estimates that approximately 10% of small entities may choose to use Level 2 as a transition step from Level 1 to Level 3. Small entities that achieve Level 1 can seek to achieve Level 3 (without first achieving a Level 2 certification) if the necessary cybersecurity practices and processes have been implemented. The Department does not anticipate releasing new contracts that require contractors to achieve CMMC Level 2. As a result, the Department did not consider alternatives with respect to CMMC Level 2.

For CMMC Level 3, the practices encompass all the 110 security requirements of NIST SP 800–171, as specified in DFARS clause 252.204–7012, as well as 13 additional cybersecurity requirements above Level 2. In addition, CMMC Level 3 includes three process maturity requirements. These additional cybersecurity practices were incorporated based upon several considerations that included public comments from September to December 2019 on draft versions of the model, inputs from the DIB Sector Coordinating Council (SCC), cybersecurity threats, the progression of cybersecurity capabilities from Level 3 to Levels 4, and other factors. The CMMC phased rollout estimates that 48,999 of the 163,325 small entities or 30% will be required to achieve CMMC Level 3. The alternatives considered include removing a subset or all of the 20 additional practices at Level 3 or moving a subset or all of the 20 additional practices from Level 3 to Level 4. The primary drawback of these alternatives is that the cybersecurity capability gaps associated with protecting CUI will not be addressed until Level 4, which will apply to a relatively small percentage of non-small and small entities. Furthermore, the progression of cybersecurity capabilities from Level 3 to Level 4 becomes more abrupt.

For CMMC Level 4, the practices encompass the 110 security requirements of NIST SP 800–171 as specified in DFARS clause 252.204–7012 and 46 additional cybersecurity requirements. More specifically, CMMC Level 4 adds 26 enhanced security requirements above CMMC Level 3, of which 13 are derived from Draft NIST SP 800–171B. In addition, CMMC Level 4 includes four process maturity requirements. The DIB SCC and the public contributed to the specification of the other 13 enhanced security requirements. For CMMC Level 4, an alternative considered is to define a threshold for contractors to meet 15 out of the 26 enhanced security requirements. In addition, contractors will be required to meet 6 out of the 11 remaining non-threshold enhanced security requirements. This alternative implies that a contractor will have to implement 21 of the 26 enhanced security requirements as well as the associated maturity processes. A drawback of this alternative is that contractors implement a different subset of the 11 non-threshold requirements which in turn, leads to a non-uniform set of cybersecurity capabilities across those certified at Level 4.

For CMMC Level 5, the practices encompass the 110 security requirements of NIST SP 800–171 as specified in DFARS clause 252.204–7012 and 61 additional cybersecurity requirements. More specifically, CMMC Level 5 adds 15 enhanced security requirements above CMMC Level 4, of which 4 are derived from Draft NIST SP 800–171B. In addition, CMMC Level 5 includes five process maturity requirements. The DIB SCC and the public contributed to the specification of the other 11 enhanced security requirements. For CMMC Level 5, the alternative considered is to define a threshold for contractors to meet 6 out of the 15 enhanced security requirements. In addition, contractors will be required to meet 5 out of the 9 remaining non-threshold enhanced security requirements. This alternative implies that a contractor will have implemented 11 of the 15 enhanced security requirements as well as the associated maturity processes. A drawback of this alternative is that contractors implement a different subset of the 9 non-threshold requirements which in turn, leads to a non-uniform set of cybersecurity capabilities across those certified at Level 5.

2. Timing of CMMC Level Certification Requirement

In addition to evaluating the make-up of the CMMC levels, the Department

took into consideration the timing of the requirement to achieve a CMMC level certification: (1) At time of proposal or offer submission, (2) in order to receive award, or (3) post contract award. The Department ultimately adopted alternative 2 to require certification at the time of award. The drawback of alternative 1 (at time of proposal or offer submission) is the increased risk for contractors since they may not have sufficient time to achieve the required CMMC certification after the release of the Request for Information (RFI). The drawback of alternative 3 (after contract award) is the increased risk to the Department with respect to the schedule and uncertainty with respect to the case where the contractor is unable to achieve the required CMMC level in a reasonable amount of time given their current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI. The Department seeks public comment on the timing of contract award, to include the effect of requiring certification at time of award on small businesses.

DoD invites comments from small business concerns and other interested parties on the expected impact of this rule on small entities. DoD will also consider comments from small entities concerning the existing regulations in subparts affected by this rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (DFARS Case 2019–D041), in correspondence.

VIII. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information, unless that collection has obtained OMB approval and displays a currently valid OMB Control Number.

DoD requested, and OMB authorized, emergency processing of the collection of information tied to this rule, as OMB Control Number 0750–0004, *Assessing Contractor Implementation of Cybersecurity Requirements,* consistent with 5 CFR 1320.13.

DoD has determined the following conditions have been met:

a. The collection of information is needed prior to the expiration of time periods normally associated with a routine submission for review under the provisions of the PRA, to enable the Department to immediately begin assessing the current status of contractor implementation of NIST SP 800–171 on their information systems that process CUI.

b. The collection of information is essential to DoD's mission. The collection of information is essential to DoD's mission. The National Defense Strategy (NDS) and DoD Cyber Strategy highlight the importance of protecting the Defense Industrial Base (DIB) to maintain national and economic security. To this end, DoD requires defense contractors and subcontractors to implement the NIST SP 800–171 security requirements on information systems that handle CUI, pursuant to DFARS clause 252.204–7012. This DoD Assessment Methodology enables the Department to assess strategically, at a corporate-level, contractor implementation of the NIST SP 800–171 security requirements. Results of a NIST SP 800–171 DoD Assessment reflect the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor.

c. Moreover, DoD cannot comply with the normal clearance procedures, because public harm is reasonably likely to result if current clearance procedures are followed. Authorizing collection of this information on the effective date will motivate defense contractors and subcontractors who have not yet implemented existing NIST SP 800–171 security requirements, to take action to implement the security requirements on covered information systems that process CUI, in order to protect our national and economic security interests. The aggregate loss of sensitive controlled unclassified information and intellectual property from the DIB sector could undermine U.S. technological advantages and increase risk to DoD missions.

Upon publication of this rule, DoD intends to provide a separate 60-day notice in the **Federal Register** requesting public comment for OMB Control Number 0750–0004, *Assessing Contractor Implementation of Cybersecurity Requirements.*

DOD estimates the annual public reporting burden for the information collection as follows:

a. Basic Assessment

Respondents: 13,068.
Responses per respondent: 1.
Total annual responses: 13,068.
Hours per response: .75.
Total burden hours: 9,801.

b. Medium Assessment

Respondents: 200.
Responses per respondent: 1.
Total annual responses: 200.
Hours per response: 8.
Total burden hours: 1,600.

c. High Assessment

Respondents: 110.
Responses per respondent: 1.
Total annual responses: 110.
Hours per response: 420.
Total burden hours: 46,200.

d. Total Public Burden (All Entities)

Respondents: 13,068.
Total annual responses: 13,378.
Total burden hours: 57,601.

e. Total Public Burden (Small Entities)

Respondents: 8,823.
Total annual responses: 9,023.
Total burden hours: 41,821.

The requirement to collect information from offerors and contractors regarding the status of their implementation of NIST SP 800–171 on their information systems that process CUI, is being imposed via a new solicitation provision and contract clause. Per the new provision, if an offeror is required to have implemented the NIST SP 800–171 security requirements on their information systems pursuant to DFARS clause 252.204–7012, then the offeror must have, at minimum, a current self-assessment (or Basic Assessment) uploaded to DoD's Supplier Performance Risk System, in order to be considered for award. Depending on the criticality of the acquisition program, after contract award, certain contractors may be required to participate in a Medium or High assessment to be conducted by DoD assessor. During these post-award assessments, contractors will be required to demonstrate their implementation of NIST SP 800–171 security requirements. Results of a NIST SP 800–171 DoD Assessment reflect the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor.

IX. Determination To Issue an Interim Rule

A determination has been made under the authority of the Secretary of Defense that urgent and compelling reasons exist to promulgate this interim rule without prior opportunity for public comment pursuant to 41 U.S.C. 1707(d) and FAR 1.501–3(b).

Malicious cyber actors have targeted, and continue to target, the DIB sector, which consists of over 200,000 small-to-large sized entities that support the warfighter. In particular, actors ranging from cyber criminals to nation-states continue to attack companies and organizations that comprise the Department's multi-tier supply chain including smaller entities at the lower

tiers. These actors seek to steal DoD's intellectual property to undercut the United States' strategic and technological advantage and to benefit their own military and economic development.

The Department has been focused on improving the cyber resiliency and security of the DIB sector for over a decade as evidenced by the development of minimum cybersecurity standards and the implementation of those standards in the National Institute of Standards and Technology (NIST) Special Publications (SP) and implementation of those standards in the FAR and DFARS. In 2013, DoD issued a final DFARS rule (78 FR 69273) that required contractors to implement a select number of security measures from NIST SP 800–53, Recommended Security Controls for Federal Information Systems and Organizations, to facilitate safeguarding unclassified DoD information within contractor information systems from unauthorized access and disclosure. In 2015, DoD issued an interim DFARS rule (80 FR 81472) requiring contractors that handle Controlled Unclassified Information (CUI) on their information systems to transition by December 31, 2017, from NIST SP 800–53 to NIST SP 800–171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. NIST SP 800–171 was not only easier to use, but also provided security requirements that greatly increases the protections of Government information in contractor information systems once implemented. And, in 2016, the FAR Council mandated the use of FAR clause 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, to require all Government contractors to implement, at minimum, some basic policies and practices to safeguard Federal Contract Information (FCI) within their information systems. Since then, the Department has been engaging with industry on improving their compliance with these exiting cybersecurity requirements and developing a framework to institutionalize cybersecurity process and practices throughout the DIB sector.

Notwithstanding the fact that these minimum cybersecurity standards have been in effect on DoD contracts since as early as 2013, several surveys and questionnaires by defense industrial associations have highlighted the DIB sector's continued challenges in achieving broad implementation of these security requirements. In a 2017 questionnaire, contractors and subcontractors that responded acknowledged implementation rates of 38% to 54% for at least 10 of the 110 security requirements of NIST SP 800–171.[1] In a separate 2018 survey, 36% of contractors who responded indicated a lack of awareness of DFARS clause 252.204–7012 and 45% of contractors acknowledged not having read NIST SP 800–171.[2] In a 2019 survey, contractors that responded rated their level of preparedness for a Defense Contract Management Agency standard assessment of contractor implementation of NIST SP 800–171 at 56%.[3] Furthermore, for the High Assessments conducted on-site by DoD to date, only 36% of contractors demonstrated implementation of all 110 of the NIST SP 800–171 security requirements.

Although these industry surveys represent a small sample of the DIB sector, the results were reinforced by the findings from DoD Inspector General report in 2019 (DODIG–2019–105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take immediate steps to assess a contractor's ability to protect this information. The report emphasizes that malicious actors can exploit the vulnerabilities of contractors' networks and systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies.

Defense contractors must begin viewing cybersecurity as a part of doing business, in order to protect themselves and to protect national security. The various industry surveys and Government assessments conducted to date illustrate the following: Absent a requirement for defense contractors to demonstrate implementation of standard cybersecurity processes and practices, cybersecurity requirements will not be fully implemented, leaving DoD and the DIB unprotected and vulnerable to malicious cyber activity. To this end, section 1648 of the NDAA for FY 2020 (Pub. L. 116–92) directed the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. defense industrial base no later than February 1, 2020. In the Senate Armed Services Committee Report to accompany the NDAA for FY 2020, the Committee expressed concern that DIB contractors are an inviting target for our adversaries, who have been conducting cyberattacks to steal critical military technologies.

Developing a framework to enhance the cybersecurity of the defense industrial base will serve as an important first step toward securing the supply chain. Pursuant to section 1648, DoD has developed the CMMC Framework, which gives the Department a mechanism to certify the cyber posture of its largest defense contractors to the smallest firms in our supply chain, who have become primary targets of malicious cyber activity.

This rule is an important part of the cybersecurity framework,[4] and builds on the existing FAR and DFARS clause cybersecurity requirements by (1) adding a mechanism to immediately begin assessing the current status of contractor implementation of NIST SP 800–171 on their information systems that process CUI; and (2) to require contractors and subcontractors to take steps to fully implement existing cybersecurity requirements, plus additional processes and practices, to protect FCI and CUI on their information systems in preparation for verification under the CMMC Framework. There is an urgent need for DoD to immediately begin assessing where vulnerabilities in its supply chain exist and take steps to correct such deficiencies, which can be accomplished by requiring contractors and subcontractors that handle DoD CUI on their information systems to complete a NIST SP 800–171 Basic Assessment. In fact, while this rule includes a delayed effective date, contractors and subcontractors that are required to implement NIST SP 800–171 pursuant to DFARS clause 252.204–7012, are encouraged to immediately conduct and submit a self-assessment as described in this rule to facilitate the Department's assessment.

It is equally urgent for the Department to ensure DIB contractors that have not fully implemented the basic safeguarding requirements under FAR clause 52.204–21 or the NIST SP 800–171 security requirements pursuant to DFARS 252.204–7012 begin correcting these deficiencies immediately. These are cybersecurity requirements contractors and subcontractors should have already implemented (or in the

[1] Aerospace Industries Association. "Complying with NIST 800–171." Fall 2017.

[2] National Defense Industrial Association (NDIA). "Implementing Cybersecurity in DoD Supply Chains." White Paper. July 2018.

[3] NDIA. "Beyond Obfuscation: The Defense Industry's Position within Federal Cybersecurity Policy." A Report of the NDIA Policy Department. October 2018. Page 20 and page 24.

[4] Section 1648 of the NDAA for FY 2020 mandates the formulation of "unified cybersecurity . . . regulations . . . to be imposed on the defense industrial base for the purpose of assessing the cybersecurity of individual contractors,"

case of implementation of NIST SP 800–171, have plans of action to correct deficiencies) on information systems that handle CUI. Under the CMMC Framework, a contractor is able to achieve CMMC Level 1 Certification if they can demonstrate implementation of the basic safeguarding requirements in the FAR clause. Similarly, a contractor is able to achieve CMMC Level 3 if they can demonstrate implementation of the NIST SP 800–171 security requirements, plus some additional processes and practices. This rule ensures contractors and subcontractors focus on full implementation of existing cybersecurity requirements on their information systems and expedites the Department's ability to secure its supply chain.

For the foregoing reasons, pursuant to 41 U.S.C. 1707(d), DoD finds that urgent and compelling circumstances make compliance with the notice and comment requirements of 41 U.S.C. 1707(a) impracticable, and invokes the exception to those requirements under 41 U.S.C. 1707(d) and FAR 1.501–3(b).[5] While a public comment process will not be completed prior to the rule's effective date, DoD has incorporated feedback solicited through extensive outreach already undertaken pursuant to section 1648(d) of the NDAA for FY 2020, including through public meetings and extensive industry outreach conducted over the past year. However, pursuant to 41 U.S.C. 1707 and FAR 1.501–3(b), DoD will consider public comments received in response to this interim rule in the formation of the final rule.

List of Subjects in 204, 212, 217, and 252

Government procurement.

Jennifer D. Johnson,

Regulatory Control Officer, Defense Acquisition Regulations System.

Therefore, 48 CFR parts 204, 212, 217, and 252 are amended as follows:

■ 1. The authority citation for 48 CFR parts 204, 212, 217, and 252 continues to read as follows:

Authority: 41 U.S.C. 1303 and 48 CFR chapter 1.

[5] FAR 1.501–3(b) states that "[a]dvance comments need not be solicited when urgent and compelling circumstances make solicitation of comments impracticable prior to the effective date of the coverage, such as when a new statute must be implemented in a relatively short period of time. In such case, the coverage shall be issued on a temporary basis and shall provide for at least a 30 day public comment period."

PART 204—ADMINISTRATIVE MATTERS

■ 2. Amend section 204.7302 by revising paragraph (a) to read as follows:

204.7302 Policy.

(a)(1) Contractors and subcontractors are required to provide adequate security on all covered contractor information systems.

(2) Contractors required to implement NIST SP 800–171, in accordance with the clause at 252.204–7012, Safeguarding Covered Defense Information and Cyber incident Reporting, are required at time of award to have at least a Basic NIST SP 800–171 DoD Assessment that is current (*i.e.*, not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204–7019).

(3) The NIST SP 800–171 DoD Assessment Methodology is located at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

(4) High NIST SP 800–171 DoD Assessments will be conducted by Government personnel using NIST SP 800–171A, "Assessing Security Requirements for Controlled Unclassified Information."

(5) The NIST SP 800–171 DoD Assessment will not duplicate efforts from any other DoD assessment or the Cybersecurity Maturity Model Certification (CMMC) (see subpart 204.75), except for rare circumstances when a re-assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance.

* * * * *

■ 3. Revise section 204.7303 to read as follows:

204.7303 Procedures.

(a) Follow the procedures relating to safeguarding covered defense information at PGI 204.7303.

(b) The contracting officer shall verify that the summary level score of a current NIST SP 800–171 DoD Assessment (*i.e.*, not more than 3 years old, unless a lesser time is specified in the solicitation) (see 252.204–7019) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted in Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*), prior to—

(1) Awarding a contract, task order, or delivery order to an offeror or contractor that is required to implement NIST SP 800–171 in accordance with the clause at 252.204–7012; or

(2) Exercising an option period or extending the period of performance on a contract, task order, or delivery order with a contractor that is that is required to implement the NIST SP 800–171 in accordance with the clause at 252.204–7012.

■ 4. Amend section 204.7304 by revising the section heading and adding paragraphs (d) and (e) to read as follows:

204.7304 Solicitation provisions and contract clauses.

* * * * *

(d) Use the provision at 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(e) Use the clause at 252.204–7020, NIST SP 800–171 DoD Assessment Requirements, in all solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for those that are solely for the acquisition of COTS items.

■ 5. Add subpart 204.75, consisting of 204.7500 through 204.7503, to read as follows:

Subpart 204.75—Cybersecurity Maturity Model Certification

Sec.

Subpart 204.75—Cybersecurity Maturity Model Certification

204.7500 Scope of subpart.

(a) This subpart prescribes policies and procedures for including the Cybersecurity Maturity Model Certification (CMMC) level requirements in DoD contracts. CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see *https://www.acq.osd.mil/cmmc/index.html*).

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information,

nor does it affect requirements of the National Industrial Security Program.

204.7501 Policy.

(a) The contracting officer shall include in the solicitation the required CMMC level, if provided by the requiring activity. Contracting officers shall not award a contract, task order, or delivery order to an offeror that does not have a current (*i.e.,* not more than 3 years old) CMMC certificate at the level required by the solicitation.

(b) Contractors are required to achieve, at time of award, a CMMC certificate at the level specified in the solicitation. Contractors are required to maintain a current (*i.e.,* not more than 3 years old) CMMC certificate at the specified level, if required by the statement of work or requirement document, throughout the life of the contract, task order, or delivery order. Contracting officers shall not exercise an option period or extend the period of performance on a contract, task order, or delivery order, unless the contract has a current (*i.e.,* not more than 3 years old) CMMC certificate at the level required by the contract, task order, or delivery order.

(c) The CMMC Assessments shall not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a re-assessment may be necessary such as, but not limited to when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.

204.7502 Procedures.

(a) When a requiring activity identifies a requirement for a contract, task order, or delivery order to include a specific CMMC level, the contracting officer shall not—

(1) Award to an offeror that does not have a CMMC certificate at the level required by the solicitation; or

(2) Exercise an option or extend any period of performance on a contract, task order, or delivery order unless the contractor has a CMMC certificate at the level required by the contract.

(b) Contracting officers shall use Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) to verify an offeror or contractor's CMMC level.

204.7503 Contract clause.

Use the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, as follows:

(a) Until September 30, 2025, in solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf (COTS) items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement a phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by OUSD(A&S).

(b) On or after October 1, 2025, in all solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items.

PART 212—ACQUISITION OF COMMERCIAL ITEMS

■ 6. Amend section 212.301, by adding paragraphs (f)(ii)(K), (L), and (M) to read as follows:

212.301 Solicitation provisions and contract clauses for acquisition of commercial items.

* * * * *

(f) * * *

(ii) * * *

(K) Use the provision at 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements, as prescribed in 204.7304(d).

(L) Use the clause at 252.204–7020, NIST SP 800–171 DoD Assessment Requirements, as prescribed in 204.7304(e).

(M) Use the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, as prescribed in 204.7503(a) and (b).

* * * * *

PART 217—SPECIAL CONTRACTING METHODS

■ 7. Amend section 217.207 by revising paragraph (c) to read as follows:

217.207 Exercise of options.

(c) In addition to the requirements at FAR 17.207(c), exercise an option only after:

(1) Determining that the contractor's record in the System for Award Management database is active and the contractor's Data Universal Numbering System (DUNS) number, Commercial and Government Entity (CAGE) code, name, and physical address are accurately reflected in the contract document. See PGI 217.207 for the requirement to perform cost or price analysis of spare parts prior to exercising any option for firm-fixed-price contracts containing spare parts.

(2) Verifying in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) that—

(i) The summary level score of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old, unless a lesser time is specified in the solicitation) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted (see 204.7303).

(ii) The contractor has a CMMC certificate at the level required by the contract, and that it is current (*i.e.,* not more than 3 years old) (see 204.7502).

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 8. Add sections 252.204–7019, 252.204–7020, and 252.204–7021 to read as follows:

Sec.

* * * * *

252.204–7019 Notice of NIST SP 800–171 DoD Assessment Requirements.

252.204–7020 NIST SP 800–171 DoD Assessment Requirements.

252.204–7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.

* * * * *

252.204–7019 Notice of NIST SP 800–171 DoD Assessment Requirements.

As prescribed in 204.7304(d), use the following provision:

NOTICE OF NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)

(a) *Definitions.*

Basic Assessment, Medium Assessment, and *High Assessment* have the meaning given in the clause 252.204–7020, NIST SP 800–171 DoD Assessments.

Covered contractor information system has the meaning given in the clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this solicitation.

(b) *Requirement.* In order to be considered for award, if the Offeror is required to implement NIST SP 800–171, the Offeror shall have a current assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204–7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800–171 DoD Assessments are described in the NIST SP 800–171 DoD Assessment Methodology located at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

(c) *Procedures.* (1) The Offeror shall verify that summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is

specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) for all covered contractor information systems relevant to the offer.

(2) If the Offeror does not have summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the Offeror may conduct and submit a Basic Assessment to *webptsmh@navy.mil* for posting to SPRS in the format identified in paragraph (d) of this provision.

(d) *Summary level scores.* Summary level scores for all assessments will be posted 30 days post-assessment in SPRS to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments.* An Offeror may follow the procedures in paragraph (c)(2) of this provision for posting Basic Assessments to SPRS.

(i) The email shall include the following information:

(A) Cybersecurity standard assessed (*e.g.,* NIST SP 800–171 Rev 1).

(B) Organization conducting the assessment (*e.g.,* Contractor self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and

(*2*) A brief description of the system security plan architecture, if more than one plan exists.

(D) Date the assessment was completed.

(E) Summary level score (*e.g.,* 95 out of 110, NOT the individual value for each requirement).

(F) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(ii) If multiple system security plans are addressed in the email described at paragraph (d)(1)(i) of this section, the Offeror shall use the following format for the report:

System security plan	CAGE codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total score	Date score of 110 will achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system assessed:

(i) The standard assessed (*e.g.,* NIST SP 800–171 Rev 1).

(ii) Organization conducting the assessment, *e.g.,* DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) A brief description of the system security plan architecture, if more than one system security plan exists.

(v) Date and level of the assessment, *i.e.,* medium or high.

(vi) Summary level score (*e.g.,* 105 out of 110, not the individual value assigned for each requirement).

(vii) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(3) *Accessibility.* (i) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(ii) Authorized representatives of the Offeror for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.*

(iii) A High NIST SP 800–171 DoD Assessment may result in documentation in addition to that listed in this section. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (*e.g.,* Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(End of provision)

252.204–7020 NIST SP 800–171 DoD Assessment Requirements.

As prescribed in 204.7304(e), use the following clause:

NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)

(a) *Definitions.*

Basic Assessment means a contractor's self-assessment of the contractor's implementation of NIST SP 800–171 that—

(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);

(2) Is conducted in accordance with the NIST SP 800–171 DoD Assessment Methodology; and

(3) Results in a confidence level of "Low" in the resulting score, because it is a self-generated score.

Covered contractor information system has the meaning given in the clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

High Assessment means an assessment that is conducted by Government personnel using NIST SP 800–171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review;

(iii) Verification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800–171 security requirements have been implemented as described in the contractor's system security plan; and

(iv) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "High" in the resulting score.

Medium Assessment means an assessment conducted by the Government that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review; and

(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "Medium" in the resulting score.

(b) *Applicability.* This clause applies to covered contractor information systems that are required to comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, in accordance with Defense Federal Acquisition Regulation System (DFARS) clause at 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

(c) *Requirements.* The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800–171 DoD Assessment, as described in NIST SP 800–171 DoD Assessment Methodology at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html,* if necessary.

(d) *Procedures.* Summary level scores for all assessments will be posted in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) to provide DoD

Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments.* A contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800–171 DoD Assessment Methodology to *webptsmh@navy.mil* for posting to SPRS.

(i) The email shall include the following information:

(A) Version of NIST SP 800–171 against which the assessment was conducted.

(B) Organization conducting the assessment (*e.g.*, Contractor self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and

(*2*) A brief description of the system security plan architecture, if more than one plan exists.

(D) Date the assessment was completed.

(E) Summary level score (*e.g.*, 95 out of 110, NOT the individual value for each requirement).

(F) Date that all requirements are expected to be implemented (*i.e.*, a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(ii) If multiple system security plans are addressed in the email described at paragraph (b)(1)(i) of this section, the Contractor shall use the following format for the report:

System security plan	CAGE codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total score	Date score of 110 will achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system security plan assessed:

(i) The standard assessed (*e.g.*, NIST SP 800–171 Rev 1).

(ii) Organization conducting the assessment, *e.g.*, DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) A brief description of the system security plan architecture, if more than one system security plan exists.

(v) Date and level of the assessment, *i.e.*, medium or high.

(vi) Summary level score (*e.g.*, 105 out of 110, not the individual value assigned for each requirement).

(vii) Date that all requirements are expected to be implemented (*i.e.*, a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.

(e) *Rebuttals.* (1) DoD will provide Medium and High Assessment summary level scores to the Contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS (see SPRS User's Guide *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf*).

(2) Upon completion of each assessment, the contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

(f) *Accessibility.* (1) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(2) Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.*

(3) A High NIST SP 800–171 DoD Assessment may result in documentation in addition to that listed in this clause. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (*e.g.*, Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(g) *Subcontracts.* (1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).

(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800–171 security requirements, in accordance with DFARS clause 252.204–7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800–171 DoD Assessment, as described in *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html*, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

(3) If a subcontractor does not have summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.*, not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800–171 DoD Assessment Methodology, to *webptsmh@navy.mil* for posting to SPRS along with the information required by paragraph (d) of this clause.

(End of clause)

252.204–7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.

As prescribed in 204.7503(a) and (b), insert the following clause:

CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENT (NOV 2020)

(a) *Scope.* The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see *https://www.acq.osd.mil/cmmc/index.html*).

(b) *Requirements.* The Contractor shall have a current (*i.e.* not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

(c) *Subcontracts.* The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (*i.e.*, not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

(End of clause)

[FR Doc. 2020–21123 Filed 9–28–20; 8:45 am]

BILLING CODE 5001–06–P

RIN Data

FAR **RIN:** 9000-AN56 **Publication ID:** Spring 2017

Title: ●Federal Acquisition Regulation (FAR); FAR Case 2017-016, Controlled Unclassified Information (CUI)

Abstract:

DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation (FAR) to implement the National Archives and Records Administration (NARA) Controlled Unclassified Information (CUI) program of Executive Order 13556 of Nov 4, 2010. As the executive agent designated to oversee the governmentwide CUI program, NARA issued implementing regulations in late 2016 designed to address agency policies for designating, safeguarding, disseminating, marking, decontrolling and disposing of CUI. The NARA rule affects contractors that handle, possess, use, share or receive CUI. The NARA regulation is codified at 32 CFR 2002. This FAR rule is necessary to ensure uniform implementation of the requirements of the CUI program in contracts across the government, thereby avoiding potentially inconsistent agency-level action.

Agency: DOD/GSA/NASA (FAR)(FAR)

Priority: Other Significant

RIN Status: First time published in the Unified Agenda

Agenda Stage of Rulemaking: Proposed Rule Stage

Major: No

Unfunded Mandates: No

EO 13771 Designation:

CFR Citation: 48 CFR 4 48 CFR 52

Legal Authority: 40 U.S.C. 121(c) 10 U.S.C. ch 137 51 U.S.C. 20113

Legal Deadline: None

Timetable:

Action	Date	FR Cite
NPRM	12/00/2017	
NPRM Comment Period End	02/00/2018	

Regulatory Flexibility Analysis Required: Yes

Government Levels Affected: Federal

Small Entities Affected: Businesses

Federalism: No

Included in the Regulatory Plan: No

RIN Information URL: www.regulations.gov

Public Comment URL: www.regulations.gov

RIN Data Printed in the FR: Yes

Agency Contact:
FAR Policy
DOD/GSA/NASA (FAR)
1800 F Street, NW,
Washington, DC 20405
Phone:202 969-4075
Email: farpolicy@gsa.gov

JOHN S. MCCAIN NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2019

★ **(Star Print)**

SEC. 889. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.

41 USC 3901 note prec.

(a) PROHIBITION ON USE OR PROCUREMENT.—(1) The head of an executive agency may not—

(A) procure or obtain or extend or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system; or

(B) enter into a contract (or extend or renew a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

(2) Nothing in paragraph (1) shall be construed to—

(A) prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(B) cover telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(b) PROHIBITION ON LOAN AND GRANT FUNDS.—(1) The head of an executive agency may not obligate or expend loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain the equipment, services, or systems described in subsection (a).

(2) In implementing the prohibition in paragraph (1), heads of executive agencies administering loan, grant, or subsidy programs, including the heads of the Federal Communications Commission, the Department of Agriculture, the Department of Homeland Security, the Small Business Administration, and the Department of Commerce, shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained.

(3) Nothing in this subsection shall be construed to—

(A) prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(B) cover telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) EFFECTIVE DATES.—The prohibition under subsection (a)(1)(A) shall take effect one year after the date of the enactment of this Act, and the prohibitions under subsections (a)(1)(B) and (b)(1) shall take effect two years after the date of the enactment of this Act.

(d) WAIVER AUTHORITY.—

(1) EXECUTIVE AGENCIES.—The head of an executive agency may, on a one-time basis, waive the requirements under subsection (a) with respect to an entity that requests such a waiver. The waiver may be provided, for a period of not more than two years after the effective dates described in subsection (c), if the entity seeking the waiver—

(A) provides a compelling justification for the additional time to implement the requirements under such subsection, as determined by the head of the executive agency; and

(B) submits to the head of the executive agency, who shall not later than 30 days thereafter submit to the appropriate congressional committees, a full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the entity's supply chain and a phase-out plan to eliminate such covered telecommunications or video surveillance equipment or services from the entity's systems.

(2) DIRECTOR OF NATIONAL INTELLIGENCE.—The Director of National Intelligence may provide a waiver on a date later than the effective dates described in subsection (c) if the Director determines the waiver is in the national security interests of the United States.

(f) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees'" means—

(A) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Financial Services, the Committee on Foreign Affairs, and the Committee on Oversight and Government Reform of the House of Representatives.

(2) COVERED FOREIGN COUNTRY.—The term "covered foreign country" means the People's Republic of China.

(3) COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES.—The term "covered telecommunications equipment or services" means any of the following:

(A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

(B) For 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 (or any subsidiary or affiliate of such entities).

(C) Telecommunications or video surveillance services provided by such entities or using such equipment.

(D) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

(4) EXECUTIVE AGENCY.—The term "executive agency" has the meaning given the term in section 133 of title 41, United States Code.

SEC. 890. PILOT PROGRAM TO ACCELERATE CONTRACTING AND PRICING PROCESSES.

10 USC 2306a note.

(a) IN GENERAL.—The Secretary of Defense shall establish a pilot program to reform and accelerate the contracting and pricing processes associated with contracts in excess of $50,000,000 by—

(1) basing price reasonableness determinations on actual cost and pricing data for purchases of the same or similar products for the Department of Defense; and

(2) reducing the cost and pricing data to be submitted in accordance with section 2306a of title 10, United States Code.

(b) LIMITATION.—The pilot program authorized under subsection (a) may include no more than ten contracts, and none of the selected contracts may be part of a major defense acquisition program (as that term is defined under section 2430 of title 10, United States Code).

(c) REPORT.—Not later than January 30, 2021, the Secretary of Defense shall submit to the congressional defense committees a report on the results of the pilot program authorized under subsection (a) and an assessment of whether the program should be continued or expanded.

(d) SUNSET.—The authority to carry out the pilot program under this section shall expire on January 2, 2021.

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

Subtitle A—Office of the Secretary of Defense and Related Matters

Subtitle B—Organization and Management of Other Department of Defense Offices and Elements

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Chapter 1

[Docket No. FAR–2020–0051, Sequence No. 5]

Federal Acquisition Regulation; Federal Acquisition Circular 2020–09; Introduction

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Summary presentation of an interim rule.

SUMMARY: This document summarizes the Federal Acquisition Regulation (FAR) rule agreed to by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) in this Federal Acquisition Circular (FAC) 2020–09. A companion document, the *Small Entity Compliance Guide* (SECG), follows this FAC.

DATES: For effective date see the separate document, which follows.

FOR FURTHER INFORMATION CONTACT: *Farpolicy@gsa.gov* or call 202–969–4075. Please cite FAC 2020–09, FAR case 2019–009.

RULE LISTED IN FAC 2020–09

Subject	FAR case
Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment	2019–009

ADDRESSES: The FAC, including the SECG, is available via the internet at *https://www.regulations.gov*.

SUPPLEMENTARY INFORMATION: A summary for the FAR rule follows. For the actual revisions and/or amendments made by this FAR case, refer to the specific subject set forth in the document following this summary. FAC 2020–09 amends the FAR as follows:

Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment (FAR Case 2019–009)

This second interim rule amends the Federal Acquisition Regulation to implement section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115–232). The first interim rule was published July 14, 2020.

This rule reduces the information collection burden imposed on the public by making updates to the System for Award Management (SAM) to allow an offeror to represent annually, after conducting a reasonable inquiry, whether it uses covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services. The burden to the public is reduced by allowing an offeror that responds "does not" in the annual representation at 52.204–26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v)(2)(ii) of 52.212–3, Offeror Representations and Certifications—Commercial Items, to skip the offer-by-offer representation for paragraph (d)(2) within the provision at 52.204–24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment. The provision at 52.204–26 requires that offerors review SAM prior to completing their required representations.

This rule applies to all acquisitions, including acquisitions at or below the simplified acquisition threshold and to acquisitions of commercial items, including commercially available off-the-shelf items. It may have a significant economic impact on a substantial number of small entities.

William F. Clark,

Director, Office of Government-wide Acquisition Policy, Office of Acquisition Policy, Office of Government-wide Policy.

Federal Acquisition Circular (FAC) 2020–09 is issued under the authority of the Secretary of Defense, the Administrator of General Services, and the Administrator of National Aeronautics and Space Administration.

Unless otherwise specified, all Federal Acquisition Regulation (FAR) and other directive material contained in FAC 2020–09 is effective August 27, 2020 except for FAR Case 2019–009, which is effective October 26, 2020.

Kim Herrington,

Acting Principal Director, Defense Pricing and Contracting, Department of Defense.

Jeffrey A. Koses,

Senior Procurement Executive/Deputy CAO, Office of Acquisition Policy, U.S. General Services Administration.

William G. Roets, II,

Acting Assistant Administrator, Office of Procurement, National Aeronautics and Space Administration.

[FR Doc. 2020–18771 Filed 8–26–20; 8:45 am]

BILLING CODE 6820–EP–P

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1, 4 and 52

[FAC 2020–09; FAR Case 2019–009; Docket No. FAR–2019–0009, Sequence No. 2]

RIN 9000–AN92

Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Interim rule.

SUMMARY: DoD, GSA, and NASA are issuing a second interim rule amending the Federal Acquisition Regulation (FAR) to require an offeror to represent annually, after conducting a reasonable inquiry, whether it uses covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services. The new annual representation in the provision implements a section of the John S. McCain National Defense Authorization Act for Fiscal Year 2019.

DATES: *Effective:* October 26, 2020.

Applicability: Contracting officers shall include the provision at FAR 52.204–26, Covered Telecommunications Equipment or Services-Representation—

- In solicitations issued on or after the effective date; and
- In solicitations issued before the effective date, provided award of the resulting contract(s) occurs on or after the effective date.

Comment date: Interested parties should submit written comments to the Regulatory Secretariat Division at one of the addresses shown below on or before October 26, 2020 to be considered in the formation of the final rule.

ADDRESSES: Submit comments in response to FAR Case 2019–009 via the Federal eRulemaking portal at *Regulations.gov* by searching for "FAR Case 2019–009". Select the link "Comment Now" that corresponds with FAR Case 2019–009. Follow the instructions provided at the "Comment Now" screen. Please include your name, company name (if any), and "FAR Case 2019–009" on your attached document. If your comment cannot be submitted using *https://www.regulations.gov,* call or email the points of contact in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions.

Instructions: Please submit comments only and cite "FAR Case 2019–009" in all correspondence related to this case. All comments received will be posted without change to *http://www.regulations.gov,* including any personal and/or business confidential information provided. To confirm receipt of your comment(s), please check *www.regulations.gov,* approximately two to three days after submission to verify posting.

All filers using the portal should use the name of the person or entity submitting comments as the name of their files, in accordance with the instructions below. Anyone submitting business confidential information should clearly identify the business confidential portion at the time of submission, file a statement justifying nondisclosure and referencing the specific legal authority claimed, and provide a non-confidential version of the submission.

Any business confidential information should be in an uploaded file that has a file name beginning with the characters "BC." Any page containing business confidential information must be clearly marked "BUSINESS CONFIDENTIAL" on the top of that page. The corresponding non-confidential version of those comments must be clearly marked "PUBLIC." The file name of the non-confidential version should begin with the character "P." The "BC" and "P" should be followed by the name of the person or entity submitting the comments or rebuttal comments. All filers should name their files using the name of the person or entity submitting the comments. Any submissions with file names that do not begin with a "BC" or "P" will be assumed to be public and will be made publicly available through *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: *Farpolicy@gsa.gov* or call 202–969–4075. Please cite FAR Case 2019–009.

SUPPLEMENTARY INFORMATION:

I. Background

The Federal Acquisition Regulations System codifies and publishes uniform policies and procedures for acquisitions by all executive agencies. The Federal Acquisition Regulations System consists of the Federal Acquisition Regulation (FAR), which is the primary document, and agency acquisition regulations, which implement or supplement the FAR.

In order to combat the national security and intellectual property threats that face the United States, section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115–232) prohibits executive agencies from entering into, or extending or renewing, a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The statute goes into effect August 13, 2020.

"Covered telecommunications equipment or services," as defined in the statute, means—

- Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
- For 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 (or any subsidiary or affiliate of such entities);
- Telecommunications or video surveillance services provided by such entities or using such equipment; or
- Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

To implement section 889(a)(1)(B) of the NDAA for FY 2019, DoD, GSA, and NASA published the first interim rule at 85 FR 42665 on July 14, 2020. The first interim rule added a representation to the provision at FAR 52.204–24(d)(2), Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment, which required offerors to represent on an offer-by-offer basis if the offeror "does" or "does not" use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services, and if it does, require the offeror to provide additional disclosures.

This second interim rule further implements section 889(a)(1)(B). It reduces burden on the public by allowing an offeror that represents "does not" in a new annual representation at FAR 52.204–26(c)(2), Covered Telecommunications Equipment or Services—Representation, or in paragraph (v)(2)(ii) of FAR 52.212–3, Offeror Representations and Certifications-Commercial Items, to skip the offer-by-offer representation within the provision at FAR 52.204–24(d)(2), Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment. Updates to the System for Award Management (SAM) were necessary to add this new annual representation and require offerors to represent annually, after conducting a reasonable inquiry, whether it uses covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services. These updates to SAM to

reduce the burden of the first interim rule were not available by the effective date of the first interim rule; therefore, these updates are being made in this interim rule.

SAM is used by anyone interested in the business of the Federal Government, including—

- Entities (contractors, Federal assistance recipients, and other potential award recipients) who need to register to do business with the Government, look for opportunities or assistance programs, or report subcontract information;
- Government contracting and grants officials responsible for activities with contracts, grants, past performance reporting and suspension and debarment activities;
- Public users searching for Government business information.

Representations and Certifications are FAR requirements that anyone wishing to apply for Federal contracts must complete. Representations and Certifications require entities to represent or certify to a variety of statements ranging from environmental rules compliance to entity size representation.

Agencies use the SAM entity registration information to verify recipient compliance with requirements. This reduces the duplicative practice of contractors filling out in full all the representations and certifications on an offer-by-offer basis. Instead the representations and certifications may be filled out annually and electronically.

Offerors shall consult SAM to validate whether the equipment or services they are using are from an entity providing equipment or services listed in the definition of "covered telecommunications equipment or services." The offerors will conduct a reasonable inquiry as to whether they use covered telecommunications equipment or services or any equipment, system, or service that uses covered telecommunications equipment or services.

II. Discussion and Analysis

This second interim rule adds an annual representation to the FAR at 52.204–26, Covered Telecommunications Equipment or Services—Representation, paragraph (c)(2), which requires an offeror to represent, after conducting a reasonable inquiry, whether it "does" or "does not" use covered telecommunications equipment or services, or any equipment, system or service that uses covered telecommunications equipment or services. The commercial item equivalent is at paragraph (v)(2)(ii) of FAR 52.212–3, Offeror Representations and Certifications-Commercial Items. If an offeror represents it "does not," the offer-by-offer representation at FAR 52.204–24(d)(2) is not required. If the offeror represents it "does," or has not made any representation in FAR 52.204–26(c)(2) or 52.212–3(v)(2)(ii), the representation at FAR 52.204–24(d)(2) is required. The FAR 52.204–26 representation is prescribed at FAR 4.2105(c) for use in all solicitations.

The purpose of this change is to limit the requirement to represent at FAR 52.204–24(d)(2) to only offerors that use covered telecommunication equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services.

This interim rule provides procedures at FAR 4.2103 for contracting officers handling offeror representations in the provisions at FAR 52.204–24 and 52.204–26. A contracting officer may generally rely on an offeror's representation in the provisions at FAR 52.204–24 and 52.204–26 that the offeror does not use any covered telecommunication equipment or services, or use any equipment, system or service that uses covered telecommunications equipment or services, unless the contracting officer has a reason to question the representation. In such cases the contracting officer shall follow agency procedures (*e.g.*, consult the requiring activity and legal counsel).

III. Regulatory Impact Analysis Pursuant to Executive Orders 12866 and 13563

The costs and transfer impacts of section 889(a)(1)(B) are discussed in the analysis below. This analysis was developed by the FAR Council in consultation with agency procurement officials and the Office of Management and Budget (OMB). We request public comment on the costs, benefits, and transfers generated by this rule.

A. Benefits

This rule provides significant national security benefits to the general public. According to the White House article "A New National Security Strategy for a New Era", the four pillars of the National Security Strategy (NSS) are to protect the homeland, promote American prosperity, preserve peace through strength, and advance American influence.[1] The purpose of this rule is to align with the NSS pillar to protect the homeland, by protecting the homeland from the impact of Federal contractors using covered telecommunications equipment or services that present a national security concern.

The United States faces an expanding array of foreign intelligence threats by adversaries who are using increasingly sophisticated methods to harm the Nation.[2] Threats to the United States posed by foreign intelligence entities are becoming more complex and harmful to U.S. interests.[3] Foreign intelligence actors are employing innovative combinations of traditional spying, economic espionage, and supply chain and cyber operations to gain access to critical infrastructure, and steal sensitive information and industrial secrets.[4] The exploitation of key supply chains by foreign adversaries represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure.[5] The increasing reliance on foreign-owned or controlled telecommunications equipment, such as hardware or software, and services, as well as the proliferation of networking technologies may create vulnerabilities in our nation's supply chains.[6] The evolving technology landscape is likely to accelerate these trends, threatening the security and economic well-being of the American people.[7]

Since the People's Republic of China possesses advanced cyber capabilities that it actively uses against the United States, a proactive cyber approach is needed to degrade or deny these threats before they reach our nation's networks, including those of the Federal Government and its contractors. China is increasingly asserting itself by stealing U.S. technology and intellectual property in an effort to erode the United States' economic and military superiority.[8] Chinese companies, including the companies identified in this rule, are legally required to cooperate with their intelligence services.[9] China's reputation for

[1] *https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/.*

[2] National Counterintelligence Strategy of the United States of America 2020–2022.

[3] National Counterintelligence Strategy of the United States of America 2020–2022.

[4] National Counterintelligence Strategy of the United States of America 2020–2022.

[5] National Counterintelligence Strategy of the United States of America 2020–2022.

[6] National Counterintelligence Strategy of the United States of America 2020–2022.

[7] National Counterintelligence Strategy of the United States of America 2020–2022.

[8] National Counterintelligence Strategy of the United States of America 2020–2022.

[9] NATO Cooperative Cyber Defense Center of Excellence Report on Huawei, 5G and China as a Security Threat.

persistent industrial espionage and close collaboration between its government and industry in order to amass technological secrets presents additional threats for U.S. Government contractors.[10] Therefore, there is a risk that Government contractors using 5th generation wireless communications (5G) and other telecommunications technology from the companies covered by this rule could introduce a reliance on equipment that may be controlled by the Chinese intelligence services and the military in both peacetime and crisis.[11]

The 2019 Worldwide Threat Assessment of the Intelligence Community[12] highlights additional threats regarding China's cyber espionage against the U.S. Government, corporations, and allies. The U.S.-China Economic and Security Review Commission Staff Annual Reports[13] provide additional details regarding the United States' national security interests in China's extensive engagement in the U.S. telecommunications sector. In addition, the U.S. Senate Select Committee on Intelligence Open Hearing on Worldwide Threats[14] further elaborates on China's approach to gain access to the United States' sensitive technologies and intellectual property. The U.S. House of Representatives Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE[15] further identifies how the risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national security interests.

Currently, Government contractors may not consider broad national security interests of the general public when they make decisions. This rule ensures that Government contractors make decisions in accordance with public national security interests, by ensuring that, pursuant to statute, they do not use covered telecommunications equipment or services that present national security concerns. This rule will also assist contractors in mitigating supply chain risks (*e.g.*, potential theft of trade secrets and intellectual property) due to the use of covered telecommunications equipment or services.

B. Risks to Industry of Not Complying With 889

As a strictly contractual matter, an organization's failure to submit an accurate representation to the Government constitutes a breach of contract that can lead to cancellation, termination, and financial consequences.

Therefore, it is important for contractors to develop a compliance plan that will allow them to submit accurate representations to the Government in the course of their offers.

C. Contractor Actions Needed for Compliance

The interim rule published at 85 FR 42665 on July 14, 2020, provides a 6 step process for compliance. This second interim rule updates the requirements for step 1 (regulatory familiarization) and step 5 (representation) by requiring familiarization with the new representation within the provision at 52.204–26 and submitting this new representation.

D. Public Costs and Savings

During the first year after publication of the rule, contractors will need to learn about the new representation in the provision at 52.204–26 and its requirements. The DOD, GSA, and NASA (collectively referred to here as the Signatory Agencies) estimate this cost by multiplying the time required to review the regulations and guidance implementing the rule by the estimated compensation of a general manager.

To estimate the burden to Federal offerors associated with complying with the rule, the percentage of Federal contractors that will be impacted was pulled from Federal databases. According to data from the System for Award Management (SAM), as of February 2020, there were 387,967 unique vendors registered in SAM. As of September 2019, about 74% of all SAM entities registered for all awards were awarded to entities with the primary NAICS code as small; therefore, it is assumed that out of the 387,967 unique vendors registered in SAM in February 2020, 287,096 entities are unique small entities.

We estimate that this rule will also affect businesses which become Federal contractors in the future. Based on data in SAM for FY16–FY19, the Signatory Agencies anticipate there will be an average of 79,319[16] new entities registering annually in SAM, of which 74%, 58,696, are anticipated to be small businesses.

1. Time To Review the Rule

Below is a list of compliance activities related to regulatory familiarization that the Signatory Agencies anticipate will occur after issuance of the rule:

Familiarization with paragraph (c)(2) of FAR 52.204–26, Covered Telecommunications Equipment or Services—Representation. The Signatory Agencies assume that it will take all vendors who plan to submit an offer for a Federal award 8[17] hours to familiarize themselves with the representation at FAR 52.204–26, Covered Telecommunications Equipment or Services—Representation. The Signatory Agencies assume that all entities registered in SAM, or 387,967[18] entities will complete the representation as it is required in order have a current, accurate, and complete registration in SAM. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$294 million* (= 8 hours × $94.76[19] per hour × 387,967). Of the 387,967 entities impacted by this part of the rule, it is assumed that 74%[20] or 287,096 entities are unique small entities.

In subsequent years, it is estimated that these costs will be incurred by 79,319[21] new entrants each year. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$60 million* (= 8 hours × $94.76 per hour × 79,319) per year in subsequent years.

The total cost estimated to review the amendments to the provision and the clause is estimated to be *$294 million* in the first year after publication. In subsequent years, this cost is estimated to be *$60 million* annually. The FAR Council acknowledges that there is substantial uncertainty underlying these estimates.

2. Time To Complete the Representation 52.204–26

For the annual representation at FAR 52.204–26(c)(2), we assume that all entities registered in SAM will fill out the annual representation in order to

[10] NATO Cooperative Cyber Defense Center of Excellence Report on Huawei, 5G and China as a Security Threat.

[11] NATO Cooperative Cyber Defense Center of Excellence Report on Huawei, 5G and China as a Security Threat.

[12] *https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR—SSCI.pdf.*

[13] *https://www.uscc.gov/annual-reports/archives.*

[14] *https://www.intelligence.senate.gov/sites/default/files/hearings/CHRG-115shrg28947.pdf.*

[15] *https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96.*

[16] This value is based on data on new registrants in *SAM.gov* on average for FY16, FY17, FY18, and FY19.

[17] The 8 hours are an assumption based on historical familiarization hours and subject matter expert judgment.

[18] According to data from the System for Award Management (SAM), as of February 2020, there were 387,967 unique vendors registered in SAM.

[19] The rate of $94.76 assumes an FY19 GS 13 Step 5 salary (after applying a 100% adjustment for overhead and benefits to the base rate) based on subject matter judgment.

[20] As of September 2019, about 74% of all SAM entities registered for all awards were awarded to entities with the primary NAICS code as small.

[21] This value is based on data on new registrants in *SAM.gov* on average for FY16, FY17, FY18, and FY19.

maintain a current, accurate, and complete registration in SAM. It is assumed it will take 1 [22] hour to complete the annual representation. Therefore, the Signatory Agencies assumed the cost for this portion of the rule to be *$36.8 million* (= 1 hour × $94.76 [23] per hour × 387,967 [24] entities registered in SAM).

In subsequent years, we assume that all entities that register in SAM will continue to complete the representation to ensure their SAM registration is current, accurate, and complete. Therefore, it is assumed that these costs will be incurred by the 387,967 [25] entities in SAM that are required to represent at least annually. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$36.8 million* (= 1 [26] hour × $94.76 per hour × (387,967 entities)) per year in subsequent years.

The FAR Council notes that the annual representation will likely reduce the burden on the public in cases where offerors represent "does not" in the annual representation at FAR 52.204–26(c)(2), Covered Telecommunications Equipment or Services—Representation or in paragraph (v)(2)(ii) of FAR 52.212–3, Offeror Representations and Certifications-Commercial Items; offerors can skip the offer-by-offer representation within the provision at FAR 52.204–24(d)(2), Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.

There is no way for the FAR Council to know how many of the annual representations at FAR 52.204–26(c)(2), Covered Telecommunications Equipment or Services—Representation or in paragraph (v)(2)(ii) of FAR 52.212–3, Offeror Representations and Certifications-Commercial Items, will include a response of "does not", which would allow offerors to skip the offer-by-offer representation within the provision at FAR 52.204–24(c)(2), Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.

52.204–24

In the first interim rule, this provision was required for 100% of the offers submitted. For this interim rule, the FAR Council assumes that 20% of entities will no longer have to complete the offer-by-offer representation in year 1, this would result in a cost savings of *$2.2 billion* = (3 [27] hours × $94.76 per hour × (20% * 102,792 unique entities × 378 [28] responses per entity).

In subsequent years, it is assumed that more offerors will respond "does not" in the annual representation and will be able to skip the offer-by-offer representation, however, the FAR Council lacks data to estimate this. The FAR Council believes that many entities will take advantage of this flexibility in order to reduce costs, and more will take advantage of the flexibility over time. Therefore, in subsequent years we believe that there will be more cost savings generated by having an annual representation. In the first interim rule, the FAR Council estimated 26% of new entrants would need to complete the offer-by-offer representation. We assume that this rule will reduce this fraction by half. This implies that in year 2 and beyond 50% of the burden calculated in the first interim rule ($2.2 billion per year) will be eliminated due to the entities each year responding "does not" in the annual representation and skipping the offer-by-offer representations. Therefore, the cost savings is estimated to be *$1.1 billion.*

The total cost savings of the above Public Cost Estimate by adding the annual representation in Year 1 is at least (Savings − Cost: $2,200M − 331M Cost): $1.6 billion.

The total costs of the above Cost Estimate Savings by adding the annual representation in Year 2 is at least (Savings − Cost: $1,100M − $97M): $1,003 million.

The total costs savings estimate per year by adding the annual representation in subsequent years is at least (Savings − Cost $1,100M − $97M): *$1,003 million.*

The following is a summary of the total public cost savings of this rule calculated in perpetuity at a 3 and 7-percent discount rate:

Summary (billions)	Total costs
Present Value (3%)	−$34.3
Annualized Costs (3%)	−1.0
Present Value (7%)	−15.1
Annualized Costs (7%)	−1.1

The FAR Council acknowledges that there is substantial uncertainty underlying these estimates, including elements for which an estimate is unavailable given inadequate information. As more information becomes available, including through comment in response to this notice, the FAR Council will seek to update these estimates which could increase or decrease the estimated net savings.

E. Government Cost and Savings Analysis

The FAR Council anticipates significant impact to the Government as a result of implementation of section 889(a)(1)(B) of the NDAA for FY 2019. This rule seeks to reduce the overall burden.

The primary cost to the Government will be to review the new annual representation (52.204–26(c)(2)) in SAM. However, there are anticipated savings from the reduction in the number of offer-by-offer representations (52.204–24(d)(2)).

52.204–26

For the annual representation at FAR 52.204–26(c)(2), we assume that the Government will need to review the annual representation at 52.204–26(c)(2) when the representation at 52.204–24(d)(2) has not been completed by the offeror. It is estimated 80 percent of offers received will include a completed offer-by-offer representation; therefore, an estimated 20 percent of offers received will rely on the annual representation. The average total number of awards per fiscal year is 38,854,291.[29] The number of offers received for a solicitation that results in an award varies from one to hundreds. A conservative estimate is 3 offers per award. Therefore, the Signatory Agencies estimate the total number of offers the Government receives in a year is 116,562,873. As previously stated, it is estimated that 20 percent of offers received will rely on the annual representation, or 23,312,575 (= 116,562,873*20%). At 5 minutes (.083 hour) per review the total cost for year 1 and all subsequent years is estimated to be $183.4 million (= 38,854,291 × 3 × 20% × .083 × $94.76 [30]).

[22] The hours are an assumption based on subject matter expert judgment.

[23] The rate of $94.76 assumes an FY19 GS 13 Step 5 salary (after applying a 100% adjustment for overhead and benefits to the base rate) based on subject matter judgment.

[24] According to data from the System for Award Management (SAM), as of February 2020, there were 387,967 unique vendors registered in SAM.

[25] This number assumes that 79,319 both enter and exit as registrants in SAM with the average number of entities registered each year are 387,967.

[26] The hours are an assumption based on subject matter expert judgment.

[27] The hours are an assumption based on subject matter expert judgment for an offer-by-offer representation.

[28] The responses per entity is calculated by dividing the average number of annual awards in FY16–19 by the average number of unique entities awarded a contract (38,854,291 awards/102,792 unique awardees = 378).

[29] Based on FY16–19 FPDS data.

[30] The rate of $95.76 assumes an FY19 GS 13 Step5 salary (after applying a 100% adjustment for

52.204–24

In the first interim rule, this provision was required for 100% of the offers submitted. For this interim rule, the FAR Council assumes that 20% of entities will no longer have to complete the offer-by-offer representation in year 1, this would result in a cost savings of *$2.2 billion* = (20% × 3 [31] hours × $94.76 per hour × 102,792 unique entities × 378 [32] responses per entity) because the Government would have to review less representations for 52.204–24.

In subsequent years, it is assumed that fewer offerors will respond "does" in the annual representation and will be required to complete the offer-by-offer representation, however, the FAR Council lacks data to estimate this. The FAR Council believes that many entities will take advantage of this flexibility in order to reduce costs, and more will take advantage of the flexibility over time.

This implies that in year 2 and beyond 50% of the burden calculated in the first interim rule ($2.2 billion per year) will be eliminated due to the entities each year responding "does not" in the annual representation and skipping the offer-by-offer representations. Therefore, the cost savings is estimated to be *$1.1 billion.*

The total cost savings of the above Government Cost Estimate by adding the annual representation in Year 1 is at least (Savings − Cost: $2,200M − 183.4M Cost): *$2 billion.*

The total cost savings of the above Government Cost Estimate Savings by adding the annual representation in Year 2 is at least (Savings − Cost: $1,100M − $183.4M): *$0.9 billion.*

The total Government cost savings estimate per year by adding the annual representation in subsequent years is at least (Savings − Cost $1,100M − $183.4M): *$0.9 billion.*

The following is a summary of the estimated Government costs savings calculated in perpetuity at a 3 and 7-percent discount rate:

Summary (billions)	Total costs
Present Value (3%)	−$31.6
Annualized Costs (3%)	−.9
Present Value (7%)	−14.1
Annualized Costs (7%)	−1.0

overhead and benefits to the base rate) based on subject matter judgement.

[31] The hours are an assumption based on subject matter expert judgment for an offer-by-offer representation.

[32] The responses per entity is calculated by dividing the average number of annual awards in FY16–19 by the average number of unique entities awarded a contract (38,854,291 awards/102,792 unique awardees = 378).

F. Analysis of Alternatives

The FAR Council could take no further regulatory action to implement this statute. However, this alternative would not provide the more efficient implementation and enforcement of the important national security measures accomplished by this rule as detailed above in section C. As a result, we reject this alternative.

IV. Specific Questions For Comment

To understand the exact scope of this impact and how this impact could be affected in subsequent rulemaking, DoD, GSA, and NASA welcome input on the following questions regarding anticipated impact on affected parties.

- What additional information or guidance do you view as necessary to effectively comply with this rule?
- What challenges do you anticipate facing in effectively complying with this rule?

V. Applicability to Contracts at or Below the Simplified Acquisition Threshold (SAT) and for Commercial Items, Including Commercially Available Off-the-Shelf (COTS) Items

In the first interim rule, the FAR Council determined that it would not be in the best interest of the Federal Government to exempt contracts and subcontracts in amounts not greater than the SAT, commercial item contracts, and contracts for the acquisition of COTS items, from the provision of law. As the second interim rule makes only administrative changes to the process of collecting information, and does not affect the scope of applicability of the prohibition, those determinations remain applicable. This rule adds a representation to the provision at FAR 52.204–26, Covered Telecommunications Equipment or Services—Representation, in order to implement section 889(a)(1)(B) of the NDAA for FY 2019, which prohibits executive agencies from entering into, or extending or renewing, a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system on or after August 13, 2020, unless an exception applies or a waiver has been granted.

A. Applicability to Contracts at or Below the Simplified Acquisition Threshold

41 U.S.C. 1905 governs the applicability of laws to acquisitions at or below the SAT. Section 1905 generally limits the applicability of new laws when agencies are making acquisitions at or below the SAT, but provides that such acquisitions will not be exempt from a provision of law under certain circumstances, including when the FAR Council makes a written determination and finding that it would not be in the best interest of the Federal Government to exempt contracts and subcontracts in amounts not greater than the SAT from the provision of law.

B. Applicability to Contracts for the Acquisition of Commercial Items, Including Commercially Available Off-the-Shelf Items

41 U.S.C. 1906 governs the applicability of laws to contracts for the acquisition of commercial items, and is intended to limit the applicability of laws to contracts for the acquisition of commercial items. Section 1906 provides that if the FAR Council makes a written determination that it is not in the best interest of the Federal Government to exempt commercial item contracts, the provision of law will apply to contracts for the acquisition of commercial items.

Finally, 41 U.S.C. 1907 states that acquisitions of COTS items will be exempt from a provision of law unless certain circumstances apply, including if the Administrator for Federal Procurement Policy makes a written determination and finding that would not be in the best interest of the Federal Government to exempt contracts for the procurement of COTS items from the provision of law.

C. Determinations

In issuing the first interim rule, the FAR Council determined that it is in the best interest of the Government to apply the rule to contracts at or below the SAT and for the acquisition of commercial items, and the Administrator for Federal Procurement Policy determined that it is in the best interest of the Government to apply that rule to contracts for the acquisition of COTS items. The changes made in this rule are administrative changes to the process of collecting required information, and do not alter those determinations.

VI. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of

harmonizing rules, and of promoting flexibility. This rule has been designated a "significant regulatory action" under E.O. 12866. Accordingly, the OMB has reviewed this rule. This second interim rule is a major rule under 5 U.S.C. 804.

VII. Executive Order 13771

This rule is subject to the requirements of E.O. 13771. The final rule designation, as regulatory or deregulatory under E.O. 13771, will be informed by the comments received from this interim rule. Details of estimates of costs or savings can be found in section III of this preamble.

VIII. Regulatory Flexibility Act

For the first interim rule, DoD, GSA, and NASA performed an Initial Regulatory Flexibility Analysis (IRFA).

Although the second interim rule would on aggregate reduce burdens, DoD, GSA, and NASA expect that this rule may have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.* An Initial Regulatory Flexibility Analysis (IRFA) has been performed, and is summarized as follows:

The reason for this second interim rule is to further implement section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115–232) by allowing offerors to represent annually whether they use any covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

The objective of the rule is to provide an information collection mechanism that relies on an annual representation, thereby reducing the burden of providing information, in some cases, that is required to enable agencies to determine and ensure that they are complying with section 889(a)(1)(B). The legal basis for the rule is section 889(a)(1)(B) of the NDAA for FY 2019, which prohibits executive agencies from entering into, or extending or renewing, a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, on or after August 13, 2020, unless an exception applies or a waiver has been granted.

To estimate the burden to Federal offerors associated with complying with the rule, the percentage of Federal contractors that will be impacted was pulled from Federal databases. According to data from the System for Award Management (SAM), as of February 2020, there were 387,967 unique vendors registered in SAM. As of September 2019, about 74 percent of all SAM entities registered for all awards were awarded to entities with the primary NAICS code as small; therefore, it is assumed that out of the 387,967 unique vendors registered in SAM in February 2020, 287,096 entities are unique small entities. We assume that all entities registered in SAM will fill out the annual representation because they are required to fill it out to have a current, accurate, and complete SAM registration.

The solicitation provision at 52.204–26 is prescribed for use in all solicitations. The second interim rule adds a representation at paragraph (c)(2) which requires each vendor to represent, at least annually, that it "does" or "does not" use covered telecommunications equipment or services, or any equipment, system or service that uses covered telecommunications equipment or services. Offerors shall consult the System for Award Management (SAM) to validate whether the equipment or services they are using are from an entity providing equipment or services listed in the definition of "covered telecommunications equipment or services." The offerors will conduct a reasonable inquiry as to whether they use covered telecommunications equipment or services or any equipment, system, or service that uses covered telecommunications equipment or services.

The rule does not duplicate, overlap, or conflict with any other Federal rules.

It is not possible to establish different compliance or reporting requirements or timetables that take into account the resources available to small entities or to exempt small entities from coverage of the rule, or any part thereof. DoD, GSA, and NASA were unable to identify any alternatives that would reduce the burden on small entities and still meet the objectives of section 889.

The Regulatory Secretariat Division has submitted a copy of this IRFA to the Chief Counsel for Advocacy of the Small Business Administration. A copy may be obtained from the Regulatory Secretariat Division upon request. DoD, GSA, and NASA invite comments from small business concerns and other interested parties on the expected impact of this rule on small entities.

DoD, GSA, and NASA will also consider comments from small entities concerning the existing regulations in subparts affected by the rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (FAR Case 2019–009) in correspondence.

IX. Paperwork Reduction Act

As part of the first interim rule, the FAR Council was granted emergency processing of a collection currently approved under OMB control number 9000–0201, Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment.

In the first interim rule, the burden consisted of an offer-by-offer representation at FAR 52.204–24(d)(2) to identify whether an offeror does or does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services, and a report of identified covered telecommunications equipment and services during contract performance, as required by FAR 52.204–25. In this second interim rule, the burden consists of a representation at FAR 52.204–26(c)(2) to identify whether an offeror does or does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services, and a representation at FAR 52.204–24(d)(2) to identify whether an offeror uses any equipment, system, or service that uses covered telecommunications equipment or services for each offer, unless the offeror selects "does not" in response to the provision at FAR 52.204–26(c)(2) (or its commercial item equivalent at paragraph (v)(2)(ii) of FAR 52.212–3).

With this second interim rule, this existing collection is being revised to reflect a reduction in burden.

With this change in who must complete a representation at FAR 52.204–24(d)(2), the FAR Council has estimated the number of responses required by this provision will drop from 38,854,291 to 31,083,433. With this decrease in responses needed, the burden for 52.204–24(d)(2) is expected to decrease from $11,045,497,845 to $8,836,398,333.

The representation added by this rule at 52.204–26(c)(2) is estimated to average 1 hour (the average of the time for both positive and negative representations) per response to review the prohibitions, conduct a reasonable inquiry, and complete the representation. The representation at FAR 52.204–24(d)(2) is estimated to average 3 hours (the average of the time for both positive and negative representations) per response to review the prohibitions, conduct a reasonably inquiry, and either provide a response of "does not" or provide a response of "does" and complete the additional detailed disclosure.

As part of this interim rule, the FAR Council is soliciting comments from the public in order to:

- Evaluate whether the proposed revisions to this collection of information are necessary for the proper performance of the functions of the FAR Council, including whether the information will have practical utility;

- Evaluate the accuracy of the FAR Council's estimate of the burden of the revised collection of information, including the validity of the methodology and assumptions used;
- Enhance the quality, utility, and clarity of the information to be collected; and
- Minimize the burden of the collection of information on those who are to respond including through the use of appropriate collection techniques.

Organizations and individuals desiring to submit comments on the information collection requirements associated with this rulemaking should submit comments to the Regulatory Secretariat Division (MVCB) not later than October 26, 2020 through *http://www.regulations.gov* and follow the instructions on the site. This website provides the ability to type short comments directly into the comment field or attach a file for lengthier comments. If there are difficulties submitting comments, contact the GSA Regulatory Secretariat Division at 202–501–4755 or *GSARegSec@gsa.gov*.

Instructions: All items submitted must cite Information Collection 9000–0201, Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment. Comments received generally will be posted without change to *http://www.regulations.gov*, including any personal and/or business confidential information provided. To confirm receipt of your comment(s), please check *www.regulations.gov*, approximately two to three days after submission to verify posting.

X. Determination To Issue an Interim Rule

A determination has been made under the authority of the Secretary of Defense (DoD), Administrator of General Services (GSA), and the Administrator of the National Aeronautics and Space Administration (NASA) that notice and public procedure thereon is unnecessary.

This rule is meant to mitigate risks across the supply chains that provide hardware, software, and services to the U.S. Government and further integrate national security considerations into the acquisition process. Since section 889 of the NDAA for FY 2019 was signed on August 13, 2018, the FAR Council has been working diligently to implement the statute, which has multiple effective dates embedded in section 889. Like many countries, the United States has increasingly relied on a global industrial supply chain. As threats have increased, so has the Government's scrutiny of its contractors and their suppliers. Underlying these efforts is the concern a foreign government will be able to expropriate valuable technologies, engage in espionage with regard to sensitive U.S. Government information, and/or exploit vulnerabilities in products or services. It is worth noting this rule follows a succession of other FAR and DOD rules dealing with supply chain and cybersecurity that were further described within section VI of the first interim rule published on July 14, 2020, at 85 FR 42665.

Changes necessary to the System for Award Management (SAM) to reduce the burden of the first interim rule were not available by the effective date of the rule, so in order to decrease the burden on contractors from the first rule and increase the effectiveness of the rule, the FAR Council is publishing this second interim rule on section 889(a)(1)(B).

Implementing this rule as soon as the SAM representation is available will reduce the burden on the public and the Government to comply with the critical national security regulation. Publication of a proposed rule would delay the reduction of burden and the achievement of the national security benefits that are expected from this second interim rule.

For the foregoing reasons, pursuant to 41 U.S.C. 1707(d), the FAR Council finds that urgent and compelling circumstances make compliance with the notice and comment and delayed effective date requirements of 41 U.S.C. 1707(a) and (b) impracticable, and invokes the exception to those requirements under 1707(d).

While a public comment process will not be completed prior to the rule's effective date, the FAR Council has taken into account feedback solicited through extensive outreach already undertaken, the feedback received through the two rulemakings associated with section 889(a)(1)(A), and the feedback received so far from the first interim rule published on July 14, 2020, at 85 FR 42665. The FAR Council will also consider comments submitted in response to this interim rule in issuing a subsequent rulemaking.

List of Subjects in 48 CFR Parts 1, 4, and 52

Government procurement.

William F. Clark,

Director, Office of Government-wide Acquisition Policy, Office of Acquisition Policy, Office of Government-wide Policy.

Therefore, DoD, GSA, and NASA amend 48 CFR parts 1, 4, and 52 as set forth below:

■ 1. The authority citation for 48 CFR parts 1, 4, and 52 continues to read as follows:

Authority: 40 U.S.C. 121(c); 10 U.S.C. chapter 137; and 51 U.S.C. 20113.

PART 1—FEDERAL ACQUISITION REGULATIONS SYSTEM

■ 2. In section 1.106 amend the table by adding in numerical order FAR segment entry "52.204–26" and its OMB control numbers to read as follows:

1.106 OMB approval under the Paperwork Reduction Act.

* * * * *

FAR segment	OMB control No.
* * * * *	
52.204–26	9000–0199 and 9000–0201
* * * * *	

PART 4—ADMINISTRATIVE AND INFORMATION MATTERS

■ 3. Amend section 4.2103 by revising paragraph (a)(1) to read as follows:

4.2103 Procedures.

(a) * * *

(1)(i) If the offeror selects "does not" in paragraphs (c)(1) and/or (c)(2) of the provision at 52.204–26 or in paragraphs (v)(2)(i) and/or (v)(2)(ii) of the provision at 52.212–3, the contracting officer may rely on the "does not" representation(s), unless the contracting officer has reason to question the representation. If the contracting officer has a reason to question the representation, the contracting officer shall follow agency procedures.

(ii) If the offeror selects "does" in paragraph (c)(1) of the provision at 52.204–26 or paragraph (v)(2)(i) of the provision at 52.212–3, the offeror will be required to complete the representation in paragraph (d)(1) of the provision at 52.204–24.

(iii) If the offeror selects "does" in paragraph (c)(2) of the provision at 52.204–26 or paragraph (v)(2)(ii) of the provision at 52.212–3, the offeror will be required to complete the representation in paragraph (d)(2) of the provision at 52.204–24.

* * * * *

PART 52—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 4. Amend section 52.204–24 by revising the date of provision and the introductory text to read as follows:

52.204–24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.

* * * * *

Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Oct 2020)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in paragraph (c)(1) in the provision at 52.204–26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v)(2)(i) of the provision at 52.212–3, Offeror Representations and Certifications–Commercial Items. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it "does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services" in paragraph (c)(2) of the provision at 52.204–26, or in paragraph (v)(2)(ii) of the provision at 52.212–3.

* * * * *

■ 5. Amend section 52.204–26 by—
■ a. Revising the date of the provision;
■ b. In paragraph (a), removing "has" and adding "and "reasonable inquiry" have" in its place; and
■ c. Revising paragraph (c).

The revisions read as follows:

52.204–26 Covered Telecommunications Equipment or Services—Representation.

* * * * *

Covered Telecommunications Equipment or Services—Representation (OCT 2020)

* * * * *

(c) *Representations.* (1) The Offeror represents that it [ ] does, [ ] does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(2) After conducting a reasonable inquiry for purposes of this representation, the offeror represents that it [ ] does, [ ] does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

* * * * *

■ 6. Amend section 52.212–3 by—
■ a. Revising the date of the provision;
■ b. In paragraph (a) adding the definition "Reasonable inquiry" in alphabetical order;
■ c. Removing from paragraph (v) introductory text "of Public" and adding "and section 889 (a)(1)(B) of Public" in its place; and
■ d. Revising paragraph (v)(2).

The revisions and addition read as follows:

52.212–3 Offeror Representations and Certifications—Commercial Items.

* * * * *

Offeror Representations and Certifications—Commercial Items (Oct 2020)

* * * * *

(a) * * *

Reasonable inquiry has the meaning provided in the clause 52.204–25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

* * * * *

(v) * * *

(2) The Offeror represents that—

(i) It [ ] does, [ ] does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(ii) After conducting a reasonable inquiry for purposes of this representation, that it [ ] does, [ ] does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

* * * * *

[FR Doc. 2020–18772 Filed 8–26–20; 8:45 am]

BILLING CODE P

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Chapter 1

[Docket No. FAR–2020–0051, Sequence No. 5]

Federal Acquisition Regulation; Federal Acquisition Circular 2020–09; Small Entity Compliance Guide

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Small Entity Compliance Guide.

SUMMARY: This document is issued under the joint authority of DOD, GSA, and NASA. This *Small Entity Compliance Guide* has been prepared in accordance with section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996. It consists of a summary of the rule appearing in Federal Acquisition Circular (FAC) 2020–09, which amends the Federal Acquisition Regulation (FAR). An asterisk (*) next to a rule indicates that a regulatory flexibility analysis has been prepared. Interested parties may obtain further information regarding this rule by referring to FAC 2020–09, which precedes this document. These documents are also available via the internet at *https://www.regulations.gov.*

DATES: August 27, 2020.

FOR FURTHER INFORMATION CONTACT: *Farpolicy@gsa.gov* or call 202–969–4075. Please cite FAC 2020–09, FAR case 2019–009.

RULE LISTED IN FAC 2020–09

Subject	FAR case
* Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment	2019–009

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1, 4, 13, 39, and 52

[FAC 2020–08; FAR Case 2019–009; Docket No. FAR–2019–0009, Sequence No. 1]

RIN 9000–AN92

Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Interim rule.

SUMMARY: DoD, GSA, and NASA are amending the Federal Acquisition Regulation (FAR) to implement section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115–232).

DATES:

Effective: August 13, 2020.

Applicability: Contracting officers shall include the provision at FAR 52.204–24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment and clause at FAR 52.204–25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment as prescribed—

- In solicitations issued on or after August 13, 2020, and resultant contracts; and
- In solicitations issued before August 13, 2020, provided award of the resulting contract(s) occurs on or after August 13, 2020.

Contracting officers shall modify, in accordance with FAR 1.108(d), existing indefinite delivery contracts to include the FAR clause for future orders, prior to placing any future orders.

If exercising an option or modifying an existing contract or task or delivery order to extend the period of performance, contracting officers shall include the clause. When exercising an option, agencies should consider modifying the existing contract to add the clause in a sufficient amount of time to both provide notice for exercising the option and to provide contractors with adequate time to comply with the clause.

The contracting officer shall include the provision at 52.204–24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment, in all solicitations for an order, or notices of intent to place an order, including those issued before the effective date of this rule, under an existing indefinite delivery contract.

Comment date: Interested parties should submit written comments to the Regulatory Secretariat Division at one of the addresses shown below on or before September 14, 2020 to be considered in the formation of the final rule.

ADDRESSES: Submit comments in response to FAR Case 2019–009 via the Federal eRulemaking portal at *Regulations.gov* by searching for "FAR Case 2019–009". Select the link "Comment Now" that corresponds with FAR Case 2019–009. Follow the instructions provided at the "Comment Now" screen. Please include your name, company name (if any), and "FAR Case 2019–009" on your attached document. If your comment cannot be submitted using *https://www.regulations.gov,* call or email the points of contact in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions.

Instructions: Please submit comments only and cite FAR Case 2019–009, in all correspondence related to this case. Comments received generally will be posted without change to *http://www.regulations.gov,* including any personal and/or business confidential information provided. To confirm receipt of your comment(s), please check *www.regulations.gov,* approximately two to three days after submission to verify posting.

All filers using the portal should use the name of the person or entity submitting comments as the name of their files, in accordance with the instructions below. Anyone submitting business confidential information should clearly identify the business confidential portion at the time of submission, file a statement justifying nondisclosure and referencing the specific legal authority claimed, and provide a non-confidential version of the submission.

Any business confidential information should be in an uploaded file that has a file name beginning with the characters "BC." Any page containing business confidential information must be clearly marked "BUSINESS CONFIDENTIAL" on the top of that page. The corresponding non-confidential version of those comments must be clearly marked "PUBLIC." The file name of the non-confidential version should begin with the character "P." The "BC" and "P" should be followed by the name of the person or entity submitting the comments or rebuttal comments. All filers should name their files using the name of the person or entity submitting the comments. Any submissions with file names that do not begin with a "BC" or "P" will be assumed to be public and will be made publicly available through *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: *Farpolicy@gsa.gov* or call 202–969–4075. Please cite "FAR Case 2019–009."

SUPPLEMENTARY INFORMATION:

I. Background

Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Pub. L. 115–232) prohibits executive agencies from entering into, or extending or renewing, a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The provision goes into effect August 13, 2020.

The statute covers certain telecommunications equipment and services produced or provided by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of those entities) and certain video surveillance products or telecommunications equipment and services produced or provided by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of those entities). The statute is not limited to contracting with entities that use end-products produced by those companies; it also covers the use of any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

Section 889 has two key sections, Section 889(a)(1)(A) and Section(a)(1)(B). Section (a)(1)(A) went into effect via FAR Case 2018–017 at 84 FR 40216 on August 13, 2019. The 889(a)(1)(A) rule does the following:

- It amends the FAR to include the 889(a)(1)(A) prohibition, which prohibits agencies from procuring or obtaining equipment or services that use covered telecommunications equipment or services as a substantial or essential component or critical technology. (FAR 52.204–25)
- It requires every offeror to represent prior to award whether or not it will

provide covered telecommunications equipment or services and, if so, to furnish additional information about the covered telecommunications equipment or services. (FAR 52.204–24)

- It mandates that contractors report (within one business day) any covered telecommunications equipment or services discovered during the course of contract performance. (FAR 52.204–25)

In order to decrease the burden on contractors, the FAR Council published a second interim rule for 889(a)(1)(A), at 84 FR 68314 on December 13, 2019. This rule allows an offeror that represents "does not" in the annual representation at FAR 52.204–26 to skip the offer-by-offer representation within the provision at FAR 52.204–24.

The FAR Council will address the public comments received on both previous interim rules in a subsequent rulemaking. In addition, each agency has the opportunity under 889(a)(1)(A) to issue agency-specific procedures (as they do for any acquisition-related requirement). For example, GSA issued a FAR deviation [1] where GSA categorized risk to eliminate the representations for low and medium risk GSA-funded orders placed under GSA indefinite-delivery contracts. For agency-specific procedures, please consult with the requiring agency.

This rule implements 889(a)(1)(B) and requires submission of a representation with each offer that will require all offerors to represent, after conducting a reasonable inquiry, whether covered telecommunications equipment or services are used by the offeror. DoD, GSA, and NASA recognize that some agencies may need to tailor the approach to the information collected based on the unique mission and supply chain risks for their agency.

In order to reduce the information collection burden imposed on offerors subject to the rule, DoD, GSA, and NASA are currently working on updates to the System for Award Management (SAM) to allow offerors to represent annually after conducting a reasonable inquiry. Only offerors that provide an affirmative response to the annual representation would be required to provide the offer-by-offer representation in their offers for contracts and for task or delivery orders under indefinite-delivery contracts. Similar to the initial rule for section 889(a)(1)(A), that was published as an interim rule on August 13, 2019 and was followed by a second interim rule on December 13, 2019 to update the System for Award Management, the FAR Council intends to publish a subsequent rulemaking once the updates are ready in SAM.

Overview of the Rule

This rule implements section 889 (a)(1)(B) and applies to Federal contractors' use of covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The rule seeks to avoid the disruption of Federal contractor systems and operations that could in turn disrupt the operations of the Federal Government, which relies on contractors to provide a range of support and services. The exfiltration of sensitive data from contractor systems arising from contractors' use of covered telecommunications equipment or services could also harm important governmental, privacy, and business interests. Accordingly, due to the privacy and security risks associated with using covered telecommunications equipment or services as a substantial or essential component or critical technology of any system, the prohibition applies to any use that meets the threshold described above.

It amends the following sections of the FAR:

- FAR subpart 4.21, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.
- The provision at 52.204–24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.
- The contract clause at 52.204–25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

Definitions Discussed in This Rule

This rule does not change the definition adopted in the first interim rule of "critical technology," which was included in the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) (Section 1703 of Title XVII of the NDAA for FY 2019, Pub. L. 115–232, 50 U.S.C. 4565(a)(6)(A)). The rule does not change the definitions of "Covered foreign country," "Covered telecommunications equipment or services," and "Substantial or essential component." The term offeror will continue to refer to only the entity that executes the contract.

This rule also adds new definitions for "backhaul," "interconnection arrangements," "reasonable inquiry," and "roaming," to provide clarity regarding when an exception to the prohibition applies. These terms are not currently defined in Section 889 or within the FAR. These definitions were developed based on consultation with subject matter experts as well as analyzing existing telecommunications regulations and case law.[2]

The FAR Council is considering as part of finalization of this rulemaking with an effective date no later than August 13, 2021, to expand the scope to require that the prohibition at 52.204–24(b)(2) and 52.204–25(b)(2) applies to the offeror and any affiliates, parents, and subsidiaries of the offeror that are domestic concerns, and expand the representation at 52.204–24(d)(2) so that the offeror represents on behalf of itself and any affiliates, parents, and subsidiaries of the offeror that are domestic concerns, as to whether they use covered telecommunications equipment or services. Section IV of this rule is requesting specific feedback regarding the impact of this potential change, as well as other pertinent policy questions of interest, in order to inform finalization of this and potential future subsequent rulemakings.

II. Discussion and Analysis

To implement section 889(a)(1)(B), the contract clause at 52.204–25 was amended to prohibit agencies "from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system," unless an exception applies or a waiver is granted. This prohibition applies at the prime contract level to an entity that uses any equipment, system, or service that itself uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, regardless of whether that usage is in performance of work under a Federal contract.

The 52.204–25 prohibition under section 889(a)(1)(A) will continue to flow down to all subcontractors; however, as required by statute the prohibition for section 889(a)(1)(B) will not flow down because the prime contractor is the only "entity" that the agency "enters into a contract" with, and an agency does not directly "enter into a contract" with any subcontractors, at any tier.

The rule also adds text in subpart 13.2, Actions at or Below the Micro-

[1] *https://www.acquisition.gov/gsa-deviation/supply-chain-aug13.*

[2] *See FiberTower Spectrum Holdings, LLC* v. *F.C.C.*, 782 F.3d 692, 695 (D.C. Cir. 2015); *Worldcall Interconnect, Inc.* v. *Fed. Commc'ns Comm'n*, 907 F.3d 810, 814 (Nov. 15, 2018).

Purchase Threshold, to address section 889(a)(1)(B) with regard to micro-purchases. The prohibition will apply to all FAR contracts, including micro-purchase contracts.

Representation Requirements

Representations and Certifications are requirements that anyone wishing to apply for Federal contracts must complete. They require entities to represent or certify to a variety of statements ranging from environmental rules compliance to entity size representation.

Similar to the previous rule for section 889(a)(1)(A), that was published as an interim rule on August 13, 2019, and was followed by a second interim rule on December 13, 2019, that updated the System for Award Management (SAM), the FAR Council is in the process of making updates to SAM requiring offerors to represent whether they use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services within the meaning of this rule. This rule will add a new OMB Control Number to the list at FAR 1.106 of OMB approvals under the Paperwork Reduction Act. Offerors will consult SAM to validate whether they use equipment or services listed in the definition of "covered telecommunications equipment or services" (see FAR 4.2101).

An entity may represent that it does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services within the meaning of this rule, if a reasonable inquiry by the entity does not reveal or identify any such use. A reasonable inquiry is an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity. A reasonable inquiry need not include an internal or third-party audit.

Grants

Grants are not part of this FAR based regulation and are handled separately. Please note guidance on Section 889 for grants, which are not covered by this rule, was posted for comment at *https://www.federalregister.gov/documents/2020/01/22/2019-28524/guidance-for-grants-and-agreements.*

Agency Waiver Process

Under certain circumstances, section 889(d)(1) allows the head of an executive agency to grant a one-time waiver from 889(a)(1)(B) on a case-by-case basis that will expire no later than August 13, 2022. Executive agencies must comply with the prohibition once the waiver expires. The executive agency will decide whether or not to initiate the formal waiver process based on market research and feedback from Government contractors during the acquisition process, in concert with other internal factors. The submission of an offer will mean the offeror is seeking a waiver if the offeror makes a representation that it uses covered telecommunications equipment or services as a substantial or essential component of a system, or as critical technology as part of any system and no exception applies. Once an offeror submits its offer, the contracting officer will first have to decide if a waiver is necessary to make an award and then request the offeror to provide: (1) A compelling justification for the additional time to implement the requirements under 889(a)(1)(B), for consideration by the head of the executive agency in determining whether to grant a waiver; (2) a full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the entity's supply chain; and (3) a phase-out plan to eliminate such covered telecommunications equipment or services from the entity's systems. This does not preclude an offeror from submitting this information with their offer, in advance of a contracting officer decision to initiate the formal waiver request through the head of the executive agency.

Since the formal waiver is initiated by an executive agency and the executive agency may not know if covered telecommunications equipment or service will be used as part of the supply chain until offers are received, a determination of whether a waiver should be considered may not be possible until offers are received and the executive agency analyzes the representations from the offerors.

Given the extent of information necessary for requesting a waiver, the FAR Council anticipates that any waiver would likely take at least a few weeks to obtain. Where mission needs do not permit time to obtain a waiver, agencies may reasonably choose not to initiate one and to move forward and make award to an offeror that does not require a waiver.

Currently, FAR 4.2104 directs contracting officers to follow agency procedures for initiating a waiver request. Since a waiver is based on the agency's judgment concerning particular uses of covered telecommunications equipment or services, a waiver granted for one agency will not necessarily shed light on whether a waiver is warranted in a different procurement with a separate agency. This agency waiver process would be the same for both new and existing contracts. If a waiver is granted, with respect to particular use of covered telecommunications equipment or services, the contractor will still be required to report any additional use of covered telecommunications equipment or services discovered or identified during contract performance in accordance with 52.204–25(d).

Before granting a waiver, the agency must: (1) Have designated a senior agency official for supply chain risk management, responsible for ensuring the agency effectively carries out the supply chain risk management functions and responsibilities described in law, regulation, and policy; additionally this senior agency official will serve as the primary liaison with the Federal Acquisition Security Council (FASC); (2) establish participation in an information-sharing environment when and as required by the FASC to facilitate interagency sharing of relevant supply chain risk information; and (3) notify and consult with the Office of the Director of National Intelligence (ODNI) on the issue of the waiver request: The agency may only grant the waiver request after consulting with ODNI and confirming that ODNI does not have existing information suggesting that the waiver would present a material increase in risk to U.S. national security. Agencies may satisfy the consultation requirement by making use of one or more of the following methods as made available to agencies by ODNI (as appropriate): Guidance, briefings, best practices, or direct inquiry. If the agency has met the three conditions enumerated above and intends to grant the waiver requested, the agency must notify the ODNI and the FASC 15 days prior to granting the waiver, and provide notice to the appropriate Congressional committees within 30 days of granting the waiver. The notice must include:

(1) An attestation by the agency that granting of the waiver would not, to the agency's knowledge having conducted the necessary due diligence as directed by statute and regulation, present a material increase in risk to U.S. national security; and

(2) The required full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the entity's supply chain; and

(3) The required phase-out plan to eliminate covered telecommunications or video surveillance equipment or services from the entity's systems.

The laydown described above must include a description of each category of covered telecommunications or video surveillance equipment or services discovered after a reasonable inquiry, as well as each category of equipment, system, or service used by the entity in which such covered technology is found after such an inquiry.

In the case of an emergency, including a declaration of major disaster, in which prior notice and consultation with the ODNI and prior notice to the FASC is impracticable and would severely jeopardize performance of mission-critical functions, the head of an agency may grant a waiver without meeting the notice and consultation requirements to enable effective mission critical functions or emergency response and recovery. In the case of a waiver granted in response to an emergency, the head of an agency granting the waiver must make a determination that the notice and consultation requirements are impracticable due to an emergency condition, and within 30 days of award, notify the ODNI, the FASC, and Congress of the waiver issued under emergency circumstances.

The provision of a waiver does not alter or amend any other requirements of U.S. law, including any U.S. export control laws and regulations or protections for sensitive sources and methods. In particular, any waiver issued pursuant to these regulations is not authorization by the U.S. Government to export, reexport, or transfer (in-country) items subject to the Export Administration or International Traffic in Arms Regulations (15 CFR 730–774 and 22 CFR 120–130, respectively).

Director of National Intelligence Waiver

The statute also permits the Director of National Intelligence (DNI) to provide a waiver if the Director determines one is in the national security interests of the United States.[3] The statute does not include an expiration date for the DNI waiver. This authority is separate and distinct from that granted to an agency head as outlined above.

ODNI Categorical Scenarios

Additionally, the ODNI, in consultation with the FASC, will issue on an ongoing basis, for use in informing agency waiver decisions, guidance describing categorical uses or commonly-occurring use scenarios where presence of covered telecommunications equipment or services is likely or unlikely to pose a national security risk.

Other Technical Changes

The solicitation provision at 52.204–24 has two representations, one for 889(a)(1)(A) and one for 889(a)(1)(B). This rule adds the representation for 889(a)(1)(B). The solicitation provision at 52.204–24 also has two disclosure sections, one for 889(a)(1)(A) and one for 889(a)(1)(B). This rule adds the disclosure section for 889(a)(1)(B) with separate reporting elements depending on whether the procurement is for equipment, services related to item maintenance, or services not associated with item maintenance. The reporting elements within the disclosure are different for each category because the information needed to identify whether the prohibition applies varies for these three types of procurements. This rule also administratively renumbers the paragraphs under the disclosure section. Finally, this rule will add cross-references in FAR parts 39, Acquisition of Information Technology, and to the coverage of the section 889 prohibition at FAR subpart 4.21.

Expected Impact of This Rule

The FAR Council recognizes that this rule could impact the operations of Federal contractors in a range of industries—including in the health-care, education, automotive, aviation, and aerospace industries; manufacturers that provide commercially available off-the-shelf (COTS) items; and contractors that provide building management, billing and accounting, and freight services. The rule seeks to minimize disruption to the mission of Federal agencies and contractors to the maximum extent possible, consistent with the Federal Government's ability to ensure effective implementation and enforcement of the national security measures imposed by Section 889. As set forth in Section III.C below, the FAR Council recognizes the substantial benefits that will result from this rule.

To date, there is limited information on the extent to which the various industries will be impacted by this rule implementing the statutory requirements of section 889. To better understand the potential impact of section 889 (a)(1)(B), DoD hosted a public meeting on March 2, 2020 (See 85 FR 7735) to facilitate the Department's planning for the implementation of Section 889(a)(1)(B).

NASA also hosted a Section 889 industry engagement event on January 30, 2020, to obtain additional information on the impact this prohibition will have on NASA contractors' operations and their ability to support NASA's mission.

In addition, the FAR Council hosted a public meeting on July 19, 2019, and GSA hosted an industry engagement event on November 6, 2019 (*https://interact.gsa.gov/FY19NDAASection889*) to gather additional information on how section 889 could affect GSA's business and supply chain. The presentations are located at *https://interact.gsa.gov/FY19NDAASection889*.

Please note presentations and comments from the public meetings are *not* considered public comments on this rule.

The FAR Council notes this rule is one of a series of actions with regard to section 889 and the impact and costs to all industry sectors, including COTS items manufacturers, resellers, consultants, etc. is not well understood and is still being assessed. For example, in a filing to the Federal Communications Commission, the Rural Wireless Association estimated that at least 25% of its carriers would be impacted.[4]

In addition, while the rule will be effective as of August 13, 2020, the FAR Council is seeking public comment, including, as indicated below, on the potential impact of the rule on the affected industries. After considering the comments received, a final rule will be issued, taking into account and addressing the public comments. *See* 41 U.S.C. 1707.

Industry Costs for New Representation and Scope of Section 889(a)(1)(B)

The statute includes two exceptions at 889 (a)(2)(A) and (B). The exception at 889(a)(2)(A) allows the head of executive agency to procure with an entity "to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements." The exception at 889(a)(2)(B) allows an entity to procure "telecommunications equipment that cannot route or redirect user data traffic or [cannot] permit visibility into any user data or packets that such equipment transmits or otherwise handles." The exception allowing for procurement of services that connect to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements applies only to a Government agency that is contracting with an entity to provide a service. Therefore, the exception does

[3] Sec. 889(d)(2).

[4] *https://ecfsapi.fcc.gov/file/120808175180 45/FY%202019%20NDAA%20Reply%20Comments%20-%20FINAL.pdf.*

not apply to a contractor's use of a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements. As a result, the Federal Government is prohibited from contracting with a contractor that uses covered telecommunications equipment or services to obtain backhaul services from an internet service provider, unless a waiver is granted.

III. Regulatory Impact Analysis Pursuant to Executive Orders 12866 and 13563

The costs and transfer impacts of section 889(a)(1)(B) are discussed in the analysis below. This analysis was developed by the FAR Council in consultation with agency procurement officials and OMB. We request public comment on the costs, benefits, and transfers generated by this rule.

A. Risks to Industry of Not Complying With 889

As a strictly contractual matter, an organization's failure to submit an accurate representation to the Government constitutes a breach of contract that can lead to cancellation, termination, and financial consequences.

Therefore, it is important for contractors to develop a compliance plan that will allow them to submit accurate representations to the Government in the course of their offers.

B. Contractor Actions Needed for Compliance

Adopting a robust, risk-based compliance approach will help reduce the likelihood of noncompliance. During the first year that 889(a)(1)(B) is in effect, contractors and subcontractors will need to learn about the provision and its requirements as well as develop a compliance plan. The FAR Council assumes the following steps would most likely be part of the compliance plan developed by any entity.

1. *Regulatory Familiarization.* Read and understand the rule and necessary actions for compliance.

2. *Corporate Enterprise Tracking.* The entity must determine through a reasonable inquiry whether the entity itself uses "covered telecommunications" equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This includes examining relationships with any subcontractor or supplier for which the prime contractor has a Federal contract and uses the supplier or subcontractor's "covered telecommunications" equipment or services as a substantial or essential component of any system. A reasonable inquiry is an inquiry designed to uncover any information in the entity's possession—primarily documentation or other records—about the identity of the producer or provider of covered telecommunications equipment or services used by the entity. A reasonable inquiry need not include an internal or third-party audit.

3. *Education.* Educate the entity's purchasing/procurement, and materials management professionals to ensure they are familiar with the entity's compliance plan.

4. *Cost of Removal (if the entity independently decides to).* Once use of covered equipment and services is identified, implement procedures if the entity decides to replace existing covered telecommunications equipment or services and ensure new equipment and services acquired for use by the entity are compliant.

5. *Representation.* Provide representation to the Government regarding whether the entity uses covered telecommunications equipment and services and alert the Government if use is discovered during contract performance.

6. *Cost to Develop a Phase-out Plan and Submit Waiver Information.* For entities for which a waiver will be requested, (1) develop a phase-out plan to phase-out existing covered telecommunications equipment or services, and (2) provide waiver information to the Government to include the phase-out plan and the complete laydown of the presence of the covered telecommunications equipment or services.

C. Benefits

This rule provides significant national security benefits to the general public. According to the White House article "A New National Security Strategy for a New Era", the four pillars of the National Security Strategy (NSS) are to protect the homeland, promote American prosperity, preserve peace through strength, and advance American influence.[5] The purpose of this rule is to align with the NSS pillar to protect the homeland, by protecting the homeland from the impact of Federal contractors using covered telecommunications equipment or services that present a national security concern.

The United States faces an expanding array of foreign intelligence threats by adversaries who are using increasingly sophisticated methods to harm the Nation.[6] Threats to the United States posed by foreign intelligence entities are becoming more complex and harmful to U.S. interests.[7] Foreign intelligence actors are employing innovative combinations of traditional spying, economic espionage, and supply chain and cyber operations to gain access to critical infrastructure, and steal sensitive information and industrial secrets.[8] The exploitation of key supply chains by foreign adversaries represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure.[9] The increasing reliance on foreign-owned or controlled telecommunications equipment, such as hardware or software, and services, as well as the proliferation of networking technologies may create vulnerabilities in our nation's supply chains.[10] The evolving technology landscape is likely to accelerate these trends, threatening the security and economic well-being of the American people.[11]

Since the People's Republic of China possesses advanced cyber capabilities that it actively uses against the United States, a proactive cyber approach is needed to degrade or deny these threats before they reach our nation's networks, including those of the Federal Government and its contractors. China is increasingly asserting itself by stealing U.S. technology and intellectual property in an effort to erode the United States' economic and military superiority.[12] Chinese companies, including the companies identified in this rule, are legally required to cooperate with their intelligence services.[13] China's reputation for persistent industrial espionage and close collaboration between its government and industry in order to amass technological secrets presents additional threats for U.S. Government contractors.[14] Therefore, there is a risk

[5] *https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/.*

[6] National Counterintelligence Strategy of the United States of America 2020–2022.

[7] National Counterintelligence Strategy of the United States of America 2020–2022.

[8] National Counterintelligence Strategy of the United States of America 2020–2022.

[9] National Counterintelligence Strategy of the United States of America 2020–2022.

[10] National Counterintelligence Strategy of the United States of America 2020–2022.

[11] National Counterintelligence Strategy of the United States of America 2020–2022.

[12] National Counterintelligence Strategy of the United States of America 2020–2022.

[13] NATO Cooperative Cyber Defense Center of Excellence Report on Huawei, 5G and China as a Security Threat.

[14] NATO Cooperative Cyber Defense Center of Excellence Report on Huawei, 5G and China as a Security Threat.

that Government contractors using 5th generation wireless communications (5G) and other telecommunications technology from the companies covered by this rule could introduce a reliance on equipment that may be controlled by the Chinese intelligence services and the military in both peacetime and crisis.[15]

The 2019 Worldwide Threat Assessment of the Intelligence Community[16] highlights additional threats regarding China's cyber espionage against the U.S. Government, corporations, and allies. The U.S.-China Economic and Security Review Commission Staff Annual Reports[17] provide additional details regarding the United States' national security interests in China's extensive engagement in the U.S. telecommunications sector. In addition, the U.S. Senate Select Committee on Intelligence Open Hearing on Worldwide Threats[18] further elaborates on China's approach to gain access to the United States' sensitive technologies and intellectual property. The U.S. House of Representatives Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE[19] further identifies how the risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national-security interests.

Currently, Government contractors may not consider broad national security interests of the general public when they make decisions. This rule ensures that Government contractors keep public national security interests in mind when making decisions, by ensuring that, pursuant to statute, they do not use covered telecommunications equipment or services that present national security concerns. This rule will also assist contractors in mitigating supply chain risks (*e.g.* potential theft of trade secrets and intellectual property) due to the use of covered telecommunications equipment or services.

D. Public Costs

During the first year after publication of the rule, contractors will need to learn about the provisions and its requirements. The DOD, GSA, and NASA (collectively referred to here as the Signatory Agencies) estimate this cost by multiplying the time required to review the regulations and guidance implementing the rule by the estimated compensation of a general manager.

To estimate the burden to Federal offerors associated with complying with the rule, the percentage of Federal contractors that will be impacted was pulled from Federal databases. According to data from the System for Award Management (SAM), as of February 2020, there were 387,967 unique vendors registered in SAM. As of September 2019, about 74% of all SAM entities registered for all awards were awarded to entities with the primary NAICS code as small; therefore, it is assumed that out of the 387,967 unique vendors registered in SAM in February 2020, 287,096 entities are unique small entities. According to data from the Federal Procurement Data System (FPDS), as of February 2020, there was an average of 102,792 unique Federal awardees for FY16–FY19, of which 73%, 75,112, are unique small entities. Based on data in SAM for FY16–FY19, the Signatory Agencies anticipates there will be an average of 79,319[20] new entities registering annually in SAM, of which 74%, 57,956, are anticipated to be small businesses.

We estimate that this rule will also affect businesses which become Federal contractors in the future. As stated above, we estimate that there are 79,319[21] new entrants per year.

1. Time To Review the Rule

Below is a list of compliance activities related to regulatory familiarization that the Signatory Agencies anticipate will occur after issuance of the rule:

a. *Familiarization with FAR 52.204–24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.* The Signatory Agencies assume that it will take all vendors who plan to submit an offer for a Federal award 20[22] hours to familiarize themselves with the amendment to the offer-by-offer representation at 52.204–24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment. The Signatory Agencies assume that all entities registered in SAM, or 387,967[23] entities, plan to submit an offer for a Federal award, since there is no data available on number of offerors for Federal awards. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$735 million* (= 20 hours × $94.76[24] per hour × 387,967). Of the 387,967 entities impacted by this part of the rule, it is assumed that 74%[25] or 287,096 entities are unique small entities.

In subsequent years, these costs will be incurred by 79,319[26] new entrants each year. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$150 million* (= 20 hours × $94.76 per hour × 79,319) per year in subsequent years.

b. *Familiarization with FAR 52.204–25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.* The Signatory Agencies estimate that it will take all vendors who plan to submit an offer for a Federal award 8[27] hours to familiarize themselves with the amendment to the clause at 52.204–25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. The average number of unique awardees for FY16–FY19, or 102,792[28] entities, will be impacted by this part of the rule, assuming all entities awarded Federal contracts would have to familiarize themselves with the clause. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$78 million* (= 8 hours × $94.76 per hour × 102,792). Of the 102,792 unique Federal awardees assumed to be impacted by this part of the rule, 73% or 75,038, are unique small entities.

In subsequent years, these costs are estimated will be incurred by 26%[29] of new entrants, or 20,623 entities because it is assumed that 26% of new entrants will be awarded a Federal contract and will be required to familiarize

[15] NATO Cooperative Cyber Defense Center of Excellence Report on Huawei, 5G and China as a Security Threat.

[16] *https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.*

[17] *https://www.uscc.gov/annual-reports/archives.*

[18] *https://www.intelligence.senate.gov/sites/default/files/hearings/CHRG-115shrg28947.pdf.*

[19] *https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96.*

[20] This value is based on data on new registrants in *SAM.gov* on average for FY16, FY17, FY18, and FY19.

[21] This value is based on data on new registrants in *SAM.gov* for FY19 and FY20.

[22] The 20 hours are an assumption based on historical familiarization hours and subject matter expert judgment.

[23] According to data from the System for Award Management (SAM), as of February 2020, there were 387,967 unique vendors registered in SAM.

[24] The rate of $94.76 assumes an FY19 GS 13 Step 5 salary (after applying a 100% burden to the base rate) based on subject matter judgment.

[25] As of September 2019, about 74% of all SAM entities registered for all awards were awarded to entities with the primary NAICS code as small.

[26] This value is based on data on new registrants in *SAM.gov* on average for FY16, FY17, FY18, and FY19.

[27] The 8 hours is an assumption based on historical familiarization hours and subject matter expert judgment.

[28] As of February 2020, there was an average of 102,792 unique Federal awardees for FY16–FY19.

[29] The percentage of 26% is the percentage of active entities registered in *SAM.gov* in FY20 that were awarded contracts.

themselves with the clause. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$15.6 million* (= 8 hours × $94.76 per hour × 20,623) per year in subsequent years.

The total cost estimated to review the amendments to the provision and the clause is estimated to be *$813 million* in the first year after publication. In subsequent years, this cost is estimated to be *$166 million* annually. The FAR Council acknowledges that there is substantial uncertainty underlying these estimates.

2. Time To Establish a Corporate Enterprise Tracking Tool and Verify Covered Telecom Is Not Used Within the Corporation or by the Corporation and Ensure There Are No Future Buys

In order to complete the representation, the entity must determine, by conducting a reasonable inquiry whether the entity itself uses "covered telecommunications" equipment or services. This includes a relationship with any subcontractor or supplier in which the prime contractor has a Federal contract and uses the supplier or subcontractor's "covered telecommunications equipment or services" regardless of whether that usage is in performance of work under a Federal contract. The Signatory Agencies do not have reliable data to form an estimate as to the processes vendors will adopt to conduct a reasonable inquiry or the costs, in time and other resources, for conducting such an inquiry. The Signatory Agencies intend to evaluate any information on this topic in the comments submitted by the public.

3. Time To Complete Corporate-Wide Training on Compliance Plan

The Signatory Agencies estimate that most entities have already begun to understand the impact of Section 889 (a)(1)(A) and have already educated the appropriate personnel to that part of the prohibition. Section 889 (a)(1)(B) requires a more robust training of the organization's compliance plan, which include business partners that are outside of the typical "covered telecommunications equipment or services" purchases; such as day-day office supplies. The Signatory Agencies estimate that it will take all vendors at least 4 [30] hours of training to ensure personnel understand the organization's compliance plan for tracking partners that procure "covered telecommunications equipment and services" that may be indirectly related to their respective business activities. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$147 million* (= 4 hours × $94.76 per hour × 387,967).

Of the 387,967 [31] entities impacted by this part of the rule, it is assumed that 74% or 287,096 entities are unique small entities.

In subsequent years, we assume that 50% [32] of the 79,319 [33] new entrants will incur these costs. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$15 million* (= 4 hours × $94.76 per hour× 50% × 79,319) per year in subsequent years. The FAR Council acknowledges that there is substantial uncertainty underlying these estimates.

4. Time To Remove and Replace Existing Equipment or Services (if Contractor Decides to) in Order To Be Eligible for a Federal Contract

Data on the extent of the presence of the covered telecommunications equipment and services in the global supply chain is extremely limited, as is information as to the costs of removing and replacing covered equipment or services where it does exist. Furthermore, no data exists as to how many entities will receive a 2-year waiver from executive agency heads or a non-time-limited waiver from the ODNI. Accordingly, the Signatory Agencies are unable to form any estimate of the costs of this rule with regard to removing and replacing existing equipment and services. The Signatory Agencies intend to evaluate any information provided on this topic in comments submitted by the public.

5. Time To Complete the Representation

52.204–24

For the offer-by-offer representation at FAR 52.204–24 the Signatory Agencies assumed the cost for this portion of the rule to be *$11 billion* (= 3 [34] hours × $94.76 per hour × 102,792 unique entities × 378 [35] responses per entity).

In subsequent years, we assume that 26% [36] of new entrants will complete an offer and need to complete the offer-by-offer representation. Therefore, these costs will be incurred by 26% of the 79,319 [37] new entrants each year. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$2.2 billion* (= 3 hours × $94.76 per hour × 26% × 79,319 × 378 responses per entity) per year in subsequent years.

The FAR Council notes that these costs are based on offer-by-offer representations; upon completion of the updates to SAM, offerors will be able to make annual representations, which is anticipated to reduce the burden.

52.204–25

FAR 52.204–25 requires a written report in cases where a contractor (or subcontractor to whom the clause has been flowed down) identifies or receives notification from any source that an entity in the supply chain uses any covered telecommunications equipment or services. The signatory agencies estimate that 5% [38] of the unique entities awarded a contract (5,140) will submit approximately 5 [39] written reports annually pursuant to FAR 52.204–25. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$7.3 million* (= 3 hours × $94.76 per hour × 5,140 entities × 5 responses per entity) per year in subsequent years.

In subsequent years, we assume that half of the entities impacted in year 1 will incur these costs for 52.204–25. Therefore, the Signatory Agencies calculated the total estimated cost for this part of the rule to be *$3.6 million* (= 3 hours × $94.76 per hours 2,570 entities × 5 responses per entity) per year in subsequent years.

The total estimated burden for the representation and the clause for year one is *$11 billion.* The total annual cost for both representations in subsequent years is calculated as: *$2.2 billion.* The FAR Council acknowledges that there is substantial uncertainty underlying these estimates.

[30] The hours are an assumption based on subject matter expert judgment.

[31] According to data from the System for Award Management (SAM), as of February 2020, there were 387,967 unique vendors registered in SAM.

[32] The 50% value is an assumption based on subject matter expert judgment. In the absence, to be conservative, it assumes that 50% of new entrants will decide to perform corporate-wide training.

[33] This value is based on data on new registrants in *SAM.gov* on average for FY16, FY17, FY18, and FY19.

[34] The hours are an assumption based on subject matter expert judgment.

[35] The responses per entity is calculated by dividing the average number of annual awards in FY16–19 by the average number of unique entities awarded a contract (38,854,291 awards/102,792 unique awardees = 378).

[36] The percentage of 26% is the percentage of active entities registered in *SAM.gov* in FY20 that were awarded contracts.

[37] This value is based on data on new registrants in *SAM.gov* on average for FY16, FY17, FY18, and FY19.

[38] The 5% value was derived from subject matter expert judgment.

[39] The 5 reports value was derived from subject matter expert judgment.

6. Time To Develop a Full and Complete Laydown and Phase-Out Plan To Support Waiver Requests

The calculation at #2 above captures the time to develop a full and complete laydown. There is no way to accurately estimate the time required for offerors to develop a phase-out plan or the number of offerors for which a waiver will be requested.

The total cost of the above Public Cost Estimate in Year 1 is at least: *$12 billion.*

The total cost of the above Cost Estimate in Year 2 is at least: *$2.4 billion.*

The total cost estimate per year in subsequent years is at least: *$2.4 billion.*

The following is a summary of the estimated costs calculated in perpetuity at a 3 and 7-percent discount rate:

Summary (billions)	Total costs
Present Value (3%)	$89
Annualized Costs (3%)	2.7
Present Value (7%)	43
Annualized Costs (7%)	3

The FAR Council acknowledges that there is substantial uncertainty underlying these estimates, including elements for which an estimate is unavailable given inadequate information. As more information becomes available, including through comment in response to this notice, the FAR Council will seek to update these estimates which could very likely increase the estimated costs.

E. Government Cost Analysis

The FAR Council anticipates significant impact to the Government as a result of this rule. These impacts will appear as higher costs, reduced competition, and inability to meet some mission needs. These costs are justified in light of the compelling national security objective that this rule will advance.

The primary cost to the Government will be to review the representations and to process the waiver request. The cost to review the representations uses the same variables as the cost to the public to fill out the representation resulting in a total cost to the Government of $11 billion as the hourly rate, hours to review, and number of representations are the same as the industry calculations. The other cost to the Government, is the cost to review the written reports required by the clause and the calculation uses the same variables as the cost to the public to complete the report, resulting in a total cost to the Government of $7.3 million.

Higher Costs and Reduced Competition: It is anticipated that at least three factors will each lead to the Government paying higher prices for services and products it buys: (1) Contractors will pass along some of the new costs of compliance; (2) due to anticipated compliance costs, some contractors will choose to exit the Federal market, particularly for commercial services and products and a reduced level of competition would increase prices; and (3) the risk of commercial firms choosing not to do business with the Government may be heightened in areas of high technological innovation such as digital services. In recent years, DoD and GSA, among other Departments and agencies, have placed particular emphasis on recruiting non-traditional contractors to provide emerging tech services and this rule could discourage innovative technology firms from competing on Federal Government contracts.

It is also anticipated that many Federal contractors may need to hire or contract for consultants to aid them in reviewing and updating their supply chains. Market principles suggest that this may increase the costs for such experts, making it more difficult for small businesses to afford them.

Inability to Meet Mission Needs: The Government uses Competition in Contracting Act exceptions (FAR subpart 6.3) to use sole source acquisitions to meet agency needs. These acquisitions would be impacted as offerors will also be subject to the section 889 requirements. There are industries where the Government makes up a small portion of the total market. There may be markets where the vendors will choose to no longer do business with the Government; leaving no sources to meet those specific requirements for the Government. This will reduce agencies' abilities to satisfy some mission needs.

The total cost of the above Government Cost Estimate in Year 1 is: *$11 billion.*

The total cost of the above Cost Estimate in Year 2 is: *$2.2 billion.*

The total cost estimate per year in subsequent years is: *$2.2 billion.*

The following is a summary of the estimated costs calculated in perpetuity at a 3 and 7-percent discount rate:

Summary (billions)	Total costs
Present Value (3%)	$82.5
Annualized Costs (3%)	2.5
Present Value (7%)	40
Annualized Costs (7%)	2.8

F. Analysis of Alternatives

Alternative 1: The FAR Council could take no regulatory action to implement this statute. However, this alternative would not provide any implementation and enforcement of the important national security measures imposed by the law. Moreover, the general public would not experience the benefits of improved national security resulting from the rule as detailed above in Section C. As a result, we reject this alternative.

Alternative 2: The FAR Council could provide uniform procedures for how agency waivers must be initiated and processed. The statute provides this waiver authority to the head of each executive agency. Each executive agency operates a range of programs that have unique mission needs as well as unique security concerns and vulnerabilities. Since the waiver approval process will be based on each agency's judgment concerning particular use cases, standardizing the waiver process across agencies is not feasible. We believe that this alternative would not be able to best serve the public, as it would lead to inefficient waiver determinations at agencies whose ideal waiver process differs from the best possible uniform approach. As a result, we reject this alternative.

IV. Specific Questions for Comment

To understand the exact scope of this impact and how this impact could be affected in subsequent rulemaking, DoD, GSA, and NASA welcome input on the following questions regarding anticipated impact on affected parties.

- To what extent do you currently use any equipment, system, or service that itself uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system?
- The FAR Council is considering as part of finalization of this rulemaking to expand the scope to require that the prohibition at 52.204–24(b)(2) and 52.204–25(b)(2) applies to the offeror and any affiliates, parents, and subsidiaries of the offeror that are domestic concerns, and expand the representation at 52.204–24(d)(2) so that the offeror represents on behalf of itself and any affiliates, parents, and subsidiaries of the offeror that are domestic concerns, as to represent whether they use covered telecommunications equipment or services. If the scope of rule was extended to cover affiliates, parents, and subsidiaries of the offeror that are domestic concerns, how would that

impact your ability to comply with the prohibition?

- To the extent you use any equipment, system or service that uses covered telecommunications equipment or services, how much do you estimate it would cost if you decide to cease such use to come into compliance with the rule?
- To what extent do you have insight into existing systems and their components?
- What equipment and services need to be checked to determine whether they include any covered telecommunications equipment or services?
  - What are the best processes and technology to use to identify covered telecommunications equipment or services?
  - Are there automated solutions?
- What are the challenges involved in identifying uses of covered telecommunications equipment or services (domestic, foreign and transnational) that would be prohibited by the rule?
- Do you anticipate use of any products or services that are unrelated to a service provided to the Federal Government and connects to the facilities of a third-party (*e.g.* backhaul, roaming, or interconnection arrangements) that uses covered telecommunications equipment or services?
- To what extent do you currently have direct control over existing equipment, systems, or services in use (*e.g.*, physical security systems) and their components, as contrasted with contracting for equipment, systems, or services that are used by you within meaning of the statute yet provided by a separate entity (*e.g.*, landlords)? How long will it take if you decide to remove and replace covered telecommunications equipment or services that your company uses?
- When a company identifies covered telecommunications equipment or services, what are the steps to take if you decide to replace the equipment or services?
  - What do companies do if their factory or office is located in foreign country where covered telecommunications equipment or services are prevalent and alternative solutions may be unavailable?
  - What are some best practices (*e.g.*, sourcing strategies) or technologies that can assist companies with replacing covered telecommunications equipment or services?
- Are there specific use cases in the supply chain where it would not be feasible to cease use of equipment, system(s), or services that use covered telecommunications equipment and services? Please be specific in explaining why cessation of use is not feasible.
  - Will the requirement to comply with this rule impact your willingness to offer goods and services to the Federal Government? Please be specific in describing the impact (*e.g.*, what types of products or services may no longer be offered, or offered in a modified form, and why)
  - The FAR Council recognizes there could be further costs associated with this rule (*e.g.* lost business opportunities, having to relocate a building in foreign country where there is no market alternative). What are they?
  - What additional information or guidance do you view as necessary to effectively comply with this rule?
  - What other challenges do you anticipate facing in effectively complying with this rule?
- Do you have data on the extent of the presence of covered telecommunications equipment or services? If so, please provide that data.
- Do you have data on the fully burdened cost to remove and replace covered telecommunications equipment or services, if that is a decision that you decide to make? If so, please provide that data and identify how you would revise the estimated costs in the cost analysis.

V. Applicability to Contracts at or Below the Simplified Acquisition Threshold (SAT) and for Commercial Items, Including Commercially Available Off-the-Shelf (COTS) Items

This rule does not add any new provisions or clauses. The rule does not change the applicability of existing provisions or clauses to contracts at or below the SAT and contracts for the acquisition of commercial items, including COTS items. The rule is updating the provision at FAR 52.204–24 and the clause at FAR 52.204–25 to implement section 889(a)(1)(B).

A. Applicability to Contracts at or Below the Simplified Acquisition Threshold

41 U.S.C. 1905 governs the applicability of laws to acquisitions at or below the simplified acquisition threshold (SAT). Section 1905 generally limits the applicability of new laws when agencies are making acquisitions at or below the SAT, but provides that such acquisitions will not be exempt from a provision of law under certain circumstances, including when, as in this case, the FAR Council makes a written determination and finding that it would not be in the best interest of the Federal Government to exempt contracts and subcontracts in amounts not greater than the SAT from the provision of law.

B. Applicability to Contracts for the Acquisition of Commercial Items, Including Commercially Available Off-the-Shelf Items

41 U.S.C. 1906 governs the applicability of laws to contracts for the acquisition of commercial items, and is intended to limit the applicability of laws to contracts for the acquisition of commercial items. Section 1906 provides that if the FAR Council makes a written determination that it is not in the best interest of the Federal Government to exempt commercial item contracts, the provision of law will apply to contracts for the acquisition of commercial items.

Finally, 41 U.S.C. 1907 states that acquisitions of commercially available off-the-shelf (COTS) items will be exempt from a provision of law unless certain circumstances apply, including if the Administrator for Federal Procurement Policy makes a written determination and finding that it would not be in the best interest of the Federal Government to exempt contracts for the procurement of COTS items from the provision of law.

C. Determinations

The FAR Council has determined that it is in the best interest of the Government to apply the rule to contracts at or below the SAT and for the acquisition of commercial items. The Administrator for Federal Procurement Policy has determined that it is in the best interest of the Government to apply this rule to contracts for the acquisition of COTS items.

While the law does not specifically address acquisitions of commercial items, including COTS items, there is an unacceptable level of risk for the Government in contracting with entities that use equipment, systems, or services that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This level of risk is not alleviated by the fact that the equipment or service being acquired has been sold or offered for sale to the general public, either in the same form or a modified form as sold to the Government (*i.e.*, that it is a commercial item or COTS item), nor by the small size of the purchase (*i.e.*, at or below the SAT).

VI. Interim Rule Determination and Executive Orders 12866, 13563, and 13771

A determination has been made under the authority of the Secretary of Defense (DoD), Administrator of General Services (GSA), and the Administrator of the National Aeronautics and Space Administration (NASA) that urgent and compelling circumstances necessitate that this interim rule go into effect earlier than 60 days after its publication date.

Since Section 889 of the NDAA was signed on August 13, 2018, the FAR Council has been working diligently to implement the statute, which has multiple effective dates embedded in Section 889. Like many countries, the United States has increasingly relied on a global industrial supply chain. As threats have increased, so has the Government's scrutiny of its contractors and their suppliers. Underlying these efforts is the concern a foreign government will be able to expropriate valuable technologies, engage in espionage with regard to sensitive U.S. Government information, and/or exploit vulnerabilities in products or services. It is worth noting this rule follows a succession of other FAR and DOD rules dealing with supply chain and cybersecurity.

Government agencies are already authorized to exclude certain contractors and products from specified countries. For example, Section 515 of the Consolidated Appropriations Act of 2014 required certain non-DoD agencies to conduct a supply chain risk assessment before acquiring high- or-moderate-impact information systems. The relevant agencies are required to conduct the supply chain risk assessments in conjunction with the FBI to determine whether any cyber-espionage or sabotage risk associated with the acquisition of these information systems exist, with a focus on cyber threats from companies "owned, directed, or subsidized by the People's Republic of China."

More recently, U.S. intelligence agencies raised concerns that Kaspersky Lab executives were closely tied to the Russian government, and that a Russian cybersecurity law would compel Kaspersky to help Russian intelligence agencies conduct espionage. As a result, DHS issued a Binding Operational Directive effectively barring civilian Government agencies from using the software. In the FY 2018 NDAA, Congress prohibited the entire U.S. Government from using products and services from Kaspersky or related entities. In June 2018, this prohibition was implemented as an interim rule across the U.S. Government by FAR 52.204–23.

Section 889 differs from the previous efforts in substantial ways. Unlike the blanket prohibition on agency use of goods and services from Kaspersky Labs, the prohibitions in Section 889 apply to multiple companies, and apply with slightly different characterizations to products and services from the various named companies. Additionally, section 889 contains carve-outs under which the prohibitions do not apply, further complicating interpretation and implementation of rulemaking. Finally, section 889 contains distinct prohibitions related to contracting, with the first applying to products and services purchased for use by the Government, and the second applying to use of the covered telecommunications equipment or services by contractors. Given the various provisions of Section 889, including the focus in the (a)(1)(A) prohibition on addressing risk to the Government's own use of covered telecommunications equipment and services and the shorter time period available to implement that prohibition, the FAR Council first developed and published at 84 FR 40216 on August 13, 2019, FAR Case 2018–017 to implement that prohibition. As discussed in the background section of this rule, that rule focused on products and services sold to the Government (directly or indirectly through a prime contract). Changes necessary to the System for Award Management to reduce the burden of the rule were not available by the effective date of the first rule, so in order to decrease the burden on contractors from this first rule, the FAR Council published a second interim rule on Section 889(a)(1)(A) at 84 FR 68314 on December 13, 2019. After the publication of this second rule, the FAR Council accelerated its ongoing work on the provisions of Section 889(a)(1)(B). Section 889(a)(1)(B) focuses on the Federal Government's ability to contract with companies that use the covered products or services at the requisite threshold.

Given the expansiveness and complexity of Section 889(a)(1)(B), this rule required substantial up-front analysis. As described elsewhere in the rule, all three signatory agencies held public meetings to hear directly from industry on concerns with this rule, with the first occurring in July of 2019 and the most recent occurring in March of 2020. The rule was prepared in part in the spring of 2020 as the nation began shutdown due to the COVID–19 pandemic and work across the Government was diverted to respond to the national emergency; the concentration of all available resources on the response to the pandemic very significantly delayed the Government's ability to finish the rule. These factors have left the FAR Council with insufficient time to publish the rule with 60 days before the legislatively established effective date of August 13, 2020, or to complete full public notice and comment before the rule becomes effective. As noted, however, the agencies are seeking public comment on this interim rule and will consider and address those comments.

Having an implementing regulation in place by the effective date is critically important to avoid confusion, uncertainty, and potentially substantial legal consequences for agencies and the vendor community. The statute requires contractors to identify the use of covered telecommunications equipment and services in their operations and the prohibitions will take effect on August 13, 2020. If they did so without an implementing regulation in place, contractors would have no guidance as to how to comply with the requirements of Section 889(a)(1)(B), leading to situations where contractors could refuse to contract with the Government over fears that lack of compliance could yield claims for breach of contract, or claims under the False Claims Act. Concerns of this sort were expressed during the outreach conducted by the FAR Council, with contractors expressing confusion as to the scope of the statutory prohibition, and asking for explicit guidance regarding what is required to comply with the requirement; this guidance is provided by the rule in the form of instructions regarding a reasonable inquiry and what must be represented to the Government. Absent coverage in the FAR to implement these requirements in a uniform manner as of the effective date, agencies would also be forced to implement the statute on their own, absent that unifying guidance, leading to rapidly divergent implementation paths, and creating substantial additional confusion and duplicative costs for the regulated contracting community. Publication of a proposed rule under these circumstances, while providing some indication of the direction the Government intended to take, would not provide sufficient clarity or certainty to avoid these consequences, given the complexity of the subject rule.

For the foregoing reasons, pursuant to 41 U.S.C. 1707(d), the FAR Council finds that urgent and compelling circumstances make compliance with

the notice and comment and delayed effective date requirements of 41 U.S.C. 1707(a) and (b) impracticable, and invokes the exception to those requirements under 1707(d). While a public comment process will not be completed prior to the rule's effective date, the FAR Council has incorporated feedback solicited through extensive outreach already undertaken, including through public meetings conducted over the course of nine months, and the feedback received through the two rulemakings associated with Section 889(a)(1)(A). The FAR Council will also consider comments submitted in response to this interim rule in issuing a subsequent rulemaking.

This interim rule is economically significant for the purposes of Executive Orders 12866 and 13563. This rule is not subject to the requirements of E.O. 13771 (82 FR 9339, February 3, 2017) because the benefit-cost analysis demonstrates that the regulation is anticipated to improve national security as its primary direct benefit. This rule is meant to mitigate risks across the supply chains that provide hardware, software, and services to the U.S. Government and further integrate national security considerations into the acquisition process.

The Office of Information and Regulatory Affairs (OIRA) has determined that this is a major rule under the Congressional Review Act (CRA) (5 U.S.C. 804(2)). Under the CRA (5 U.S.C. 801(a)(3)), a major rule generally may not take effect until 60 days after a report on the rule is received by Congress. As a result of the factors identified above, the FAR Council has insufficient time to prepare and complete a full public notice and comment rulemaking proceeding and to timely complete a final rule prior to the effective date of August 13, 2020. Because of the substantial additional impact to the regulated community if the rule is not in place on the effective date, the FAR Council has found good cause to forego notice and public procedure, the Council also determines, pursuant to 5 U.S.C. 808(2), that this interim rule will take effect on August 13, 2020.

Pursuant to 41 U.S.C. 1707 and FAR 1.501–3(b), DoD, GSA, and NASA will consider public comments received in response to this interim rule in the formation of the final rule.

VII. Regulatory Flexibility Act

DoD, GSA, and NASA expect that this rule may have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.* An Initial Regulatory Flexibility Analysis (IRFA) has been performed, and is summarized as follows:

The reason for this interim rule is to implement section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115–232).

The objective of the rule is to provide an information collection mechanism that relies on an offer-by-offer representation that is required to enable agencies to determine and ensure that they are complying with section 889(a)(1)(B).

The legal basis for the rule is section 889(a)(1)(B) of the NDAA for FY 2019, which prohibits the Government from entering into, or extending or renewing, a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, on or after August 13, 2020, unless an exception applies or a waiver has been granted. This prohibition applies to an entity that uses at the prime contractor level any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, regardless of whether that usage is in performance of work under a Federal contract. This prohibition does not flow-down to subcontractors.

This collection includes a burden for requiring an offeror to represent if it "does" or "does not" use any equipment, system, or service that uses covered telecommunications equipment or services.

The representation requirement being added to the FAR provision at 52.204–24 will be included in all solicitations, including solicitations for contracts with small entities and is an offer-by-offer representation. A data set was generated from the Federal Procurement Data System (FPDS) for FY 2016, 2017, 2018 and 2019 for use in estimating the number of small entities affected by this rule.

The FPDS data indicates that the Government awarded contracts to an average of 102,792 unique entities, of which 75,112 (73 percent) were small entities. DoD, GSA, and NASA estimate that the representation at 52.204–24 will impact all unique entities awarded Government contracts, of which 75,112 are small entities.

This rule amends the solicitation provision at 52.204–24 to require all vendors to represent on an offer-by-offer basis, that it "does" or "does not" use any covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services and if it does to provide an additional disclosure.

If the offeror selects "does" in the representation at 52.204–24(d)(2), the offeror is required to further disclose, per paragraph (e), substantial detail regarding the basis for selecting "does" in the representation.

This rule will impact some small businesses and their ability to provide Government services at the prime contract level, since some small entities lack the resources to efficiently update their supply chain and information systems, which may be useful to comply with the prohibition.

The rule does not duplicate, overlap, or conflict with any other Federal rules.

The FAR Council intends to publish a subsequent rulemaking to allow offerors, including small entities, to represent annually in the System for Award Management (SAM) after conducting a reasonable inquiry. Only offerors that provide an affirmative response to the annual representation would be required to provide the offer-by-offer representation at 52.204–24(d)(2). The annual representation is anticipated to reduce the burden on small entities.

The Regulatory Secretariat Division has submitted a copy of the IRFA to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the IRFA may be obtained from the Regulatory Secretariat Division. DoD, GSA, and NASA invite comments from small business concerns and other interested parties on the expected impact of this rule on small entities.

DoD, GSA, and NASA will also consider comments from small entities concerning the existing regulations in subparts affected by the rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (FAR Case 2019–009) in correspondence.

VIII. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information, unless that collection has obtained OMB approval and displays a currently valid OMB Control Number.

DoD, GSA, and NASA requested, and OMB authorized, emergency processing of the collection of information involved in this rule, consistent with 5 CFR 1320.13. DoD, GSA, and NASA have determined the following conditions have been met:

a. The collection of information is needed prior to the expiration of time periods normally associated with a routine submission for review under the provisions of the PRA, because the prohibition in section 889(a)(1)(B) goes into effect on August 13, 2020.

b. The collection of information is essential to the mission of the agencies to ensure the Federal Government complies with section 889(a)(1)(B) on the statute's effective date in order to protect the Government supply chain

from risks posed by covered telecommunications equipment or services.

c. Moreover, DoD, GSA, and NASA cannot comply with the normal clearance procedures because public harm is reasonably likely to result if current clearance procedures are followed. Authorizing collection of this information on the effective date will ensure that agencies do not enter into, extend, or renew contracts with any entity that uses equipment, systems, or services that use telecommunications equipment or services from certain named companies as a substantial or essential component or critical technology as part of any system in violation of the prohibition in section 889(a)(1)(B).

DoD, GSA, and NASA intend to provide a separate 60-day notice in the **Federal Register** requesting public comment on the information collections contained within this rule under OMB Control Number 9000–0201.

The annual public reporting burden for this collection of information is estimated as follows:

Agency: DoD, GSA, and NASA.
Type of Information Collection: New Collection.
Title of Collection: Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.
FAR Clause: 52.204–24.
Affected Public: Private Sector—Business.
Total Estimated Number of Respondents: 102,792.
Average Responses per Respondents: 378.
Total Estimated Number of Responses: 38,854,291.
Average Time (for both positive and negative representations) per Response: 3 hours.
Total Annual Time Burden: 116,562,873.

Agency: DoD, GSA, and NASA.
Type of Information Collection: New Collection.
Title of Collection: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.
FAR Clause: 52.204–25.
Affected Public: Private Sector—Business.
Total Estimated Number of Respondents: 5,140.
Average Responses per Respondents: 5.
Total Estimated Number of Responses: 25,700.
Average Time per Response: 3 hours.
Total Annual Time Burden: 77,100.

Agency: DoD, GSA, and NASA.
Type of Information Collection: New Collection.
Title of Collection: Waiver from Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.
FAR Clause: 52.204–25.
Affected Public: Private Sector—Business.
Total Estimated Number of Respondents: 20,000.
Average Responses per Respondents: 1.
Total Estimated Number of Responses: 20,000.
Average Time per Response: 160 hours.
Total Annual Time Burden: 3,200,000.

The public reporting burden for this collection of information consists of a representation to identify whether an offeror uses covered telecommunications equipment or services for each offer as required by 52.204–24 and reports of identified use of covered telecommunications equipment or services as required by 52.204–25. The representation at 52.204–24 is estimated to average 3 hours per response to review the prohibitions, research the source of the product or service, and complete the additional detailed disclosure, if applicable. Reports required by 52.204–25 are estimated to average 3 hours per response, including the time for reviewing definitions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the report.

If the Government seeks a waiver from the prohibition, the offeror will be required to provide a full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the entity's supply chain and a phase-out plan to eliminate such covered telecommunications equipment or services from the offeror's systems. There is no way to estimate the total number of waivers at this time. For the purposes of complying with the PRA analysis, the FAR Council estimates 20,000 waivers; however there is no data for the basis of this estimate. This estimate may be higher or lower once the rule is in effect.

The subsequent 60-day notice to be published by DoD, GSA, and NASA will invite public comments.

List of Subjects in 48 CFR Parts 1, 4, 13, 39, and 52

Government procurement.

William F. Clark,

Director, Office of Governmentwide Acquisition Policy, Office of Acquisition Policy, Office of Governmentwide Policy.

Therefore, DoD, GSA, and NASA are amending 48 CFR parts 1, 4, 13, 39, and 52 as set forth below:

■ 1. The authority citation for 48 CFR parts 1, 4, 13, 39, and 52 continues to read as follows:

Authority: 40 U.S.C. 121(c); 10 U.S.C. chapter 137; and 51 U.S.C. 20113.

PART 1—FEDERAL ACQUISITION REGULATIONS SYSTEM

■ 2. In section 1.106 amend the table by revising the entries for "4.21", "52.204–24" and "52.204–25" to read as follows:

1.106 OMB approval under the Paperwork Reduction Act.

* * * * *

FAR segment	OMB control No.
* * * * *	
4.21	9000–0199 and 9000–0201.
* * * * *	
52.204–24	9000–0199 and 9000–0201.
52.204–25	9000–0199 and 9000–0201
* * * * *	

PART 4—ADMINISTRATIVE AND INFORMATION MATTERS

4.2100 [Amended]

■ 3. Amend section 4.2100 by removing "paragraph (a)(1)(A)" and adding "paragraphs (a)(1)(A) and (a)(1)(B)" in its place.

■ 4. Amend section 4.2101 by adding in alphabetical order the definitions "Backhaul", "Interconnection arrangements", "Reasonable inquiry" and "Roaming" to read as follows:

4.2101 Definitions.

* * * * *

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (*e.g.*, connecting cell phones/towers to the core telephone network). Backhaul can be wireless (*e.g.*, microwave) or wired (*e.g.*, fiber optic, coaxial cable, Ethernet).

* * * * *

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (*e.g.*, connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (*e.g.*, voice,

video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

* * * * *

■ 5. Amend section 4.2102 by revising paragraphs (a) and (c) to read as follows:

4.2102 Prohibition.

(a) Prohibited equipment, systems, or services.

(1) On or after August 13, 2019, agencies are prohibited from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (b) of this section applies or the covered telecommunications equipment or services are covered by a waiver described in 4.2104.

(2) On or after August 13, 2020, agencies are prohibited from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (b) of this section applies or the covered telecommunications equipment or services are covered by a waiver described in 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

* * * * *

(c) *Contracting Officers.* Unless an exception at paragraph (b) of this section applies or the covered telecommunications equipment or service is covered by a waiver described in 4.2104, Contracting Officers shall not—

(1) Procure or obtain, or extend or renew a contract (*e.g.,* exercise an option) to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system; or

(2) Enter into a contract, or extend or renew a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

* * * * *

■ 6. Amend section 4.2103 by revising paragraph (a)(2) to read as follows:

4.2103 Procedures.

(a) * * *

(2)(i) If the offeror selects "will not" in paragraph (d)(1) of the provision at 52.204–24 or "does not" in paragraph (d)(2) of the provision at 52.204–24, the contracting officer may rely on the representations, unless the contracting officer has reason to question the representations. If the contracting officer has a reason to question the representations, the contracting officer shall follow agency procedures.

(ii) If an offeror selects "will" in paragraph (d)(1) of the provision at 52.204–24, the offeror must provide the information required by paragraph (e)(1) of the provision at 52.204–24, and the contracting officer shall follow agency procedures.

(iii) If an offeror selects "does" in paragraph (d)(2) of the provision at 52.204–24, the offeror must complete the disclosure at paragraph (e)(2) of the provision at 52.204–24, and the contracting officer shall follow agency procedures.

* * * * *

■ 7. Amend section 4.2104 by revising paragraphs (a)(1) introductory text and (a)(2), and adding paragraphs (a)(3) and (4) to read as follows:

4.2104 Waivers.

(a) * * *

(1) *Waiver.* The waiver may be provided, for a period not to extend beyond August 13, 2021 for the prohibition at 4.2102(a)(1), or beyond August 13, 2022 for the prohibition at 4.2102(a)(2), if the Government official, on behalf of the entity, seeking the waiver submits to the head of the executive agency—

* * * * *

(2) *Executive agency waiver requirements for the prohibition at 4.2102(a)(2).* Before the head of an executive agency can grant a waiver to the prohibition at 4.2102(a)(2), the agency must—

(i) Have designated a senior agency official for supply chain risk management, responsible for ensuring the agency effectively carries out the supply chain risk management functions and responsibilities described in law, regulation, and policy;

(ii) Establish participation in an information-sharing environment when and as required by the Federal Acquisition Security Council (FASC) to facilitate interagency sharing of relevant acquisition supply chain risk information;

(iii) Notify and consult with the Office of the Director of National Intelligence (ODNI) on the waiver request using ODNI guidance, briefings, best practices, or direct inquiry, as appropriate; and

(iv) Notify the ODNI and the FASC 15 days prior to granting the waiver that it intends to grant the waiver.

(3) *Waivers for emergency acquisitions.*

(i) In the case of an emergency, including a declaration of major disaster, in which prior notice and consultation with the ODNI and prior notice to the FASC is impracticable and would severely jeopardize performance of mission-critical functions, the head of an agency may grant a waiver without meeting the notice and consultation requirements under 4.2104(a)(2)(iii) and 4.2104(a)(2)(iv) to enable effective mission critical functions or emergency response and recovery.

(ii) In the case of a waiver granted in response to an emergency, the head of an agency granting the waiver must—

(A) Make a determination that the notice and consultation requirements are impracticable due to an emergency condition; and

(B) Within 30 days of award, notify the ODNI and the FASC of the waiver issued under emergency conditions in addition to the waiver notice to Congress under 4.2104(a)(4).

(4) *Waiver notice.*

(i) For waivers to the prohibition at 4.2102(a)(1), the head of the executive agency shall, not later than 30 days after approval—

(A) Submit in accordance with agency procedures to the appropriate congressional committees the full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the relevant supply chain; and

(B) The phase-out plan to eliminate such covered telecommunications or video surveillance equipment or services from the relevant systems.

(ii) For waivers to the prohibition at 4.2102(a)(2), the head of the executive agency shall, not later than 30 days after approval submit in accordance with agency procedures to the appropriate congressional committees—

(A) An attestation by the agency that granting of the waiver would not, to the agency's knowledge having conducted the necessary due diligence as directed by statute and regulation, present a material increase in risk to U.S. national security;

(B) The full and complete laydown of the presences of covered

telecommunications or video surveillance equipment or services in the relevant supply chain, to include a description of each category of covered technology equipment or services discovered after a reasonable inquiry, as well as each category of equipment, system, or service used by the entity in which such covered technology is found after conducting a reasonable inquiry; and

(C) The phase-out plan to eliminate such covered telecommunications or video surveillance equipment or services from the relevant systems.

* * * * *

PART 13—SIMPLIFIED ACQUISITION PROCEDURES

■ 8. Amend section 13.201 by redesignating paragraph (j) as (j)(1) and adding paragraph (j)(2) to read as follows:

13.201 General.

* * * * *

(j)(1) * * *

(2) On or after August 13, 2020, agencies are prohibited from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception applies or a waiver is granted (see subpart 4.21). This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

PART 39—ACQUISITION OF INFORMATION TECHNOLOGY

■ 9. Amend section 39.101 by redesignating paragraph (f) as (f)(1) and adding paragraph (f)(2) to read as follows:

39.101 Policy.

* * * * *

(f)(1) * * *

(2) On or after August 13, 2020, agencies are prohibited from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception applies or a waiver is granted (see subpart 4.21). This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

PART 52—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 10. Revise section 52.204–24 to read as follows:

52.204–24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.

As prescribed in 4.2105(a), insert the following provision:

Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (AUG 2020)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in the provision at 52.204–26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v) of the provision at 52.212–3, Offeror Representations and Certifications–Commercial Items.

(a) *Definitions.* As used in this provision-

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and *substantial or essential component* have the meanings provided in the clause 52.204–25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Prohibition.* (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (*https://www.sam.gov*) for entities excluded from receiving federal awards for "covered telecommunications equipment or services."

(d) *Representations.* The Offeror represents that—

(1) It [ ] will, [ ] will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

It [ ] does, [ ] does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) *Disclosures.* (1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered

telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

■ 11. Amend section 52.204–25 by—

■ a. Revising the date of the clause;

■ b. In paragraph (a), adding in alphabetical order the definitions "Backhaul", "Interconnection arrangements", "Reasonable inquiry" and "Roaming";

■ c. Revising paragraph (b); and

■ d. Removing from paragraph (e) "this paragraph (e)" and adding "this paragraph (e) and excluding paragraph (b)(2)" in its place.

The revisions read as follows:

52.204–25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

* * * * *

Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (AUG 2020)

(a) * * *

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (*e.g.*, connecting cell phones/towers to the core telephone network). Backhaul can be wireless (*e.g.*, microwave) or wired (*e.g.*, fiber optic, coaxial cable, Ethernet).

* * * * *

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (*e.g.*, connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (*e.g.*, voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

* * * * *

(b) *Prohibition.* (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

* * * * *

■ 12. Amend section 52.212–5 by—

■ a. Revising the date of the clause;

■ b. Removing from paragraphs (a)(3) and (e)(1)(iv) "AUG 2019" and adding "AUG 2020" in their places, respectively;

■ c. Revising the date of Alternate II; and

■ d. In Alternate II, amend paragraph (e)(1)(ii)(D) by removing "AUG 2019" and adding "AUG 2020" in its place.

The revisions read as follows:

52.212–5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Items.

* * * * *

Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Items (AUG 2020)

* * * * *

Alternate II (AUG 2020). * * *

* * * * *

■ 13. Amend section 52.213–4 by—

■ a. Revising the date of the clause;

■ b. Removing from paragraph (a)(1)(iii) "AUG 2019" and adding "AUG 2020" in its place; and

■ c. Removing from paragraph (a)(2)(viii) "JUN 2020" and adding "AUG 2020" in its place.

The revision reads as follows:

52.213–4 Terms and Conditions—Simplified Acquisitions (Other Than Commercial Items).

* * * * *

Terms and Conditions—Simplified Acquisitions (Other Than Commercial Items) (AUG 2020)

* * * * *

■ 14. Amend section 52.244–6 by—

■ a. Revising the date of the clause; and

■ b. Removing from paragraph (c)(1)(vi) "AUG 2019" and adding "AUG 2020" in its place.

The revision reads as follows:

52.244–6 Subcontracts for Commercial Items.

* * * * *

Subcontracts for Commercial Items (AUG 2020)

* * * * *

[FR Doc. 2020–15293 Filed 7–13–20; 8:45 am]

BILLING CODE 6820–EP–P

Public Law 116–207
116th Congress

An Act

To establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes.

Dec. 4, 2020
[H.R. 1668]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

Internet of Things Cybersecurity Improvement Act of 2020.
15 USC 271 note.

This Act may be cited as the "Internet of Things Cybersecurity Improvement Act of 2020" or the "IoT Cybersecurity Improvement Act of 2020".

SEC. 2. SENSE OF CONGRESS.

15 USC 278g–3a note.

It is the sense of Congress that—

(1) ensuring the highest level of cybersecurity at agencies in the executive branch is the responsibility of the President, followed by the Director of the Office of Management and Budget, the Secretary of Homeland Security, and the head of each such agency;

(2) this responsibility is to be carried out by working collaboratively within and among agencies in the executive branch, industry, and academia;

(3) the strength of the cybersecurity of the Federal Government and the positive benefits of digital technology transformation depend on proactively addressing cybersecurity throughout the acquisition and operation of Internet of Things devices by the Federal Government; and

(4) consistent with the second draft National Institute for Standards and Technology Interagency or Internal Report 8259 titled "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline", published in January 2020, Internet of Things devices are devices that—

(A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and

(B) can function on their own and are not only able to function when acting as a component of another device, such as a processor.

SEC. 3. DEFINITIONS.

15 USC 278g–3a.

In this Act:

(1) AGENCY.—The term "agency" has the meaning given that term in section 3502 of title 44, United States Code.

(2) DIRECTOR OF OMB.—The term "Director of OMB" means the Director of the Office of Management and Budget.

(3) DIRECTOR OF THE INSTITUTE.—The term "Director of the Institute" means the Director of the National Institute of Standards and Technology.

(4) INFORMATION SYSTEM.—The term "information system" has the meaning given that term in section 3502 of title 44, United States Code.

(5) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given that term in section 3552(b)(6) of title 44, United States Code.

(6) OPERATIONAL TECHNOLOGY.—The term "operational technology" means hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise.

(7) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

(8) SECURITY VULNERABILITY.—The term "security vulnerability" has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)).

15 USC 278g–3b.

SEC. 4. SECURITY STANDARDS AND GUIDELINES FOR AGENCIES ON USE AND MANAGEMENT OF INTERNET OF THINGS DEVICES.

(a) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY DEVELOPMENT OF STANDARDS AND GUIDELINES FOR USE OF INTERNET OF THINGS DEVICES BY AGENCIES.—

Deadline. Publication.

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of the Institute shall develop and publish under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) standards and guidelines for the Federal Government on the appropriate use and management by agencies of Internet of Things devices owned or controlled by an agency and connected to information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices.

(2) CONSISTENCY WITH ONGOING EFFORTS.—The Director of the Institute shall ensure that the standards and guidelines developed under paragraph (1) are consistent with the efforts of the National Institute of Standards and Technology in effect on the date of the enactment of this Act—

(A) regarding—

(i) examples of possible security vulnerabilities of Internet of Things devices; and

(ii) considerations for managing the security vulnerabilities of Internet of Things devices; and

(B) with respect to the following considerations for Internet of Things devices:

(i) Secure Development.

(ii) Identity management.

(iii) Patching.

(iv) Configuration management.

(3) CONSIDERING RELEVANT STANDARDS.—In developing the standards and guidelines under paragraph (1), the Director

of the Institute shall consider relevant standards, guidelines, and best practices developed by the private sector, agencies, and public-private partnerships.

(b) REVIEW OF AGENCY INFORMATION SECURITY POLICIES AND PRINCIPLES.—

(1) REQUIREMENT.—Not later than 180 days after the date on which the Director of the Institute completes the development of the standards and guidelines required under subsection (a), the Director of OMB shall review agency information security policies and principles on the basis of the standards and guidelines published under subsection (a) pertaining to Internet of Things devices owned or controlled by agencies (excluding agency information security policies and principles pertaining to Internet of Things of devices owned or controlled by agencies that are or comprise a national security system) for consistency with the standards and guidelines submitted under subsection (a) and issue such policies and principles as may be necessary to ensure those policies and principles are consistent with such standards and guidelines. Deadline.

(2) REVIEW.—In reviewing agency information security policies and principles under paragraph (1) and issuing policies and principles under such paragraph, as may be necessary, the Director of OMB shall—

(A) consult with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security; and Consultation.

(B) ensure such policies and principles are consistent with the information security requirements under subchapter II of chapter 35 of title 44, United States Code.

(3) NATIONAL SECURITY SYSTEMS.—Any policy or principle issued by the Director of OMB under paragraph (1) shall not apply to national security systems.

(c) QUINQUENNIAL REVIEW AND REVISION.— Deadlines.

(1) REVIEW AND REVISION OF NIST STANDARDS AND GUIDELINES.—Not later than 5 years after the date on which the Director of the Institute publishes the standards and guidelines under subsection (a), and not less frequently than once every 5 years thereafter, the Director of the Institute, shall—

(A) review such standards and guidelines; and

(B) revise such standards and guidelines as appropriate.

(2) UPDATED OMB POLICIES AND PRINCIPLES FOR AGENCIES.—Not later than 180 days after the Director of the Institute makes a revision pursuant to paragraph (1), the Director of OMB, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall update any policy or principle issued under subsection (b)(1) as necessary to ensure those policies and principles are consistent with the review and any revision under paragraph (1) under this subsection and paragraphs (2) and (3) of subsection (b). Consultation.

(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement any standards and guidelines promulgated in this section.

15 USC 278g–3c.

SEC. 5. GUIDELINES ON THE DISCLOSURE PROCESS FOR SECURITY VULNERABILITIES RELATING TO INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

Deadline. Consultation. Publication.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Institute, in consultation with such cybersecurity researchers and private sector industry experts as the Director considers appropriate, and in consultation with the Secretary, shall develop and publish under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) guidelines—

(1) for the reporting, coordinating, publishing, and receiving of information about—

(A) a security vulnerability relating to information systems owned or controlled by an agency (including Internet of Things devices owned or controlled by an agency); and

(B) the resolution of such security vulnerability; and

(2) for a contractor providing to an agency an information system (including an Internet of Things device) and any subcontractor thereof at any tier providing such information system to such contractor, on—

(A) receiving information about a potential security vulnerability relating to the information system; and

(B) disseminating information about the resolution of a security vulnerability relating to the information system.

(b) ELEMENTS.—The guidelines published under subsection (a) shall—

(1) to the maximum extent practicable, be aligned with industry best practices and Standards 29147 and 30111 of the International Standards Organization (or any successor standard) or any other appropriate, relevant, and widely-used standard;

(2) incorporate guidelines on—

(A) receiving information about a potential security vulnerability relating to an information system owned or controlled by an agency (including an Internet of Things device); and

(B) disseminating information about the resolution of a security vulnerability relating to an information system owned or controlled by an agency (including an Internet of Things device); and

(3) be consistent with the policies and procedures produced under section 2009(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m)).

(c) INFORMATION ITEMS.—The guidelines published under subsection (a) shall include example content, on the information items that should be reported, coordinated, published, or received pursuant to this section by a contractor, or any subcontractor thereof at any tier, providing an information system (including Internet of Things device) to the Federal Government.

(d) OVERSIGHT.—The Director of OMB shall oversee the implementation of the guidelines published under subsection (a).

Consultation.

(e) OPERATIONAL AND TECHNICAL ASSISTANCE.—The Secretary, in consultation with the Director of OMB, shall administer the implementation of the guidelines published under subsection (a) and provide operational and technical assistance in implementing such guidelines.

SEC. 6. IMPLEMENTATION OF COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

Consultation.
15 USC 278g–3d.

(a) AGENCY GUIDELINES REQUIRED.—Not later than 2 years after the date of the enactment of this Act, the Director of OMB, in consultation with the Secretary, shall develop and oversee the implementation of policies, principles, standards, or guidelines as may be necessary to address security vulnerabilities of information systems (including Internet of Things devices). Deadline.

(b) OPERATIONAL AND TECHNICAL ASSISTANCE.—Consistent with section 3553(b) of title 44, United States Code, the Secretary, in consultation with the Director of OMB, shall provide operational and technical assistance to agencies on reporting, coordinating, publishing, and receiving information about security vulnerabilities of information systems (including Internet of Things devices).

(c) CONSISTENCY WITH GUIDELINES FROM NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—The Secretary shall ensure that the assistance provided under subsection (b) is consistent with applicable standards and publications developed by the Director of the Institute.

(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement the provisions under this section.

SEC. 7. CONTRACTOR COMPLIANCE WITH COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INTERNET OF THINGS DEVICES.

15 USC 278g–3e.

(a) PROHIBITION ON PROCUREMENT AND USE.—

(1) IN GENERAL.—The head of an agency is prohibited from procuring or obtaining, renewing a contract to procure or obtain, or using an Internet of Things device, if the Chief Information Officer of that agency determines during a review required by section 11319(b)(1)(C) of title 40, United States Code, of a contract for such device that the use of such device prevents compliance with the standards and guidelines developed under section 4 or the guidelines published under section 5 with respect to such device. Determination.

(2) SIMPLIFIED ACQUISITION THRESHOLD.—Notwithstanding section 1905 of title 41, United States Code, the requirements under paragraph (1) shall apply to a contract or subcontract in amounts not greater than the simplified acquisition threshold. Applicability.

(b) WAIVER.—

(1) AUTHORITY.—The head of an agency may waive the prohibition under subsection (a)(1) with respect to an Internet of Things device if the Chief Information Officer of that agency determines that— Determination.

(A) the waiver is necessary in the interest of national security;

(B) procuring, obtaining, or using such device is necessary for research purposes; or

(C) such device is secured using alternative and effective methods appropriate to the function of such device.

(2) AGENCY PROCESS.—The Director of OMB shall establish a standardized process for the Chief Information Officer of each agency to follow in determining whether the waiver under paragraph (1) may be granted.

(c) REPORTS TO CONGRESS.—

Time period.

(1) REPORT.—Every 2 years during the 6-year period beginning on the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate a report—

(A) on the effectiveness of the process established under subsection (b)(2);

Recommendations.

(B) that contains recommended best practices for the procurement of Internet of Things devices; and

Lists.

Time period.

(C) that lists—

(i) the number and type of each Internet of Things device for which a waiver under subsection (b)(1) was granted during the 2-year period prior to the submission of the report; and

(ii) the legal authority under which each such waiver was granted, such as whether the waiver was granted pursuant to subparagraph (A), (B), or (C) of such subsection.

(2) CLASSIFICATION OF REPORT.—Each report submitted under this subsection shall be submitted in unclassified form, but may include a classified annex that contains the information described under paragraph (1)(C).

(d) EFFECTIVE DATE.—The prohibition under subsection (a)(1) shall take effect 2 years after the date of the enactment of this Act.

SEC. 8. GOVERNMENT ACCOUNTABILITY OFFICE REPORT ON CYBERSECURITY CONSIDERATIONS STEMMING FROM THE CONVERGENCE OF INFORMATION TECHNOLOGY, INTERNET OF THINGS, AND OPERATIONAL TECHNOLOGY DEVICES, NETWORKS, AND SYSTEMS.

Deadline.

(a) BRIEFING.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall provide a briefing to the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate on broader Internet of Things efforts, including projects designed to assist in managing potential security vulnerabilities associated with the use of traditional information technology devices, networks, and systems with—

(1) Internet of Things devices, networks, and systems; and

(2) operational technology devices, networks, and systems.

(b) REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General shall submit a report to the

Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate on broader Internet of Things efforts addressed in subsection (a).

Approved December 4, 2020.

LEGISLATIVE HISTORY—H.R. 1668 (S. 734):

HOUSE REPORTS: No. 116–501, Pt. 1 (Comm. on Oversight and Reform).
SENATE REPORTS: No. 116–112 (Comm. on Homeland Security and Governmental Affairs) accompanying S. 734.
CONGRESSIONAL RECORD, Vol. 166 (2020):
Sept. 14, considered and passed House.
Nov. 17, considered and passed Senate.