



August 1, 2019

Dominic Lackey
Contracting Officer
General Services Administration
1800 F Street NW
Washington, D.C. 20405

Subject: Comments on Draft Request for Proposals (RFP) 47QSCC19R0429 – Commercial Platforms Initiative

Dear Mr. Lackey,

Coalition for Government Procurement (Coalition) members appreciate the opportunity to provide comments on the Draft Request for Proposals (RFP) 47QSCC19R0429 - Commercial Platforms Initiative issued by the General Services Administration (GSA) on July 2, 2019.

The Coalition is a non-profit association of firms selling commercial services and products to the Federal Government. Its members collectively account for a significant percentage of the sales generated through GSA contracts, including the Multiple Award Schedule (MAS) program. Coalition members also are responsible for many of the commercial item solutions purchased annually by the Federal Government. These members include small, medium, and large business concerns. The Coalition is proud to have collaborated with Government officials for 40 years in promoting the mutual goal of common-sense acquisition.

Coalition members have appreciated the opportunities to engage with GSA and the Office of Federal Procurement Policy (OFPP) on the effort to implement Section 846 of the National Defense Authorization Act (NDAA) for Fiscal Year 2018 (Section 846). Unfortunately, Coalition members find few, if any, of their fundamental issues remediated in the Draft RFP. The Coalition is most concerned about the threshold decision to identify a subset of portal solutions in the commercial e-Commerce market and conduct a “proof of concept” focusing on only one of those solutions, specifically, the portal solution. The e-marketplace model presents a higher cost to the government than existing government programs and carries the most risk to the stability of government and private sector markets.

Our comprehensive comments, provided on behalf of our members, are attached. In summary, **the Coalition recommends that GSA suspend the implementation of the proof of concept until it is revised to:**

1. **Update the draft RFP to include an assessment of all types of commercial e-Commerce solutions, as was intended by statute.** An in-depth comparative analysis of existing commercial solutions that spans the scope of at least the three models GSA identified in its Phase I report (e-marketplace, e-commerce and e-procurement) is critical to ensuring that procurement through commercial e-commerce portals is implemented consistent with Section 846 of the National

Defense Authorization Act of FY2018 (Section 846). It is unclear how the Government can properly assess which model best meets the objectives of Section 846 at a best value to taxpayers without allowing for competition *between* various e-commerce portals and assessing the performance of each model in the context of the proof of concept. Limiting the pilot to only the e-marketplace model limits competition and restricts the Government's access to the vast innovations and competitive pricing available via other existing commercial models. This pro-competition recommendation will allow the Government to effectively assess how commercial e-commerce portals can be implemented to serve government mission needs and how the government can leverage, to the maximum extent practicable, the competitive forces of the market.

2. **Apply the estimated value of the \$30 billion CPI contract at the contract level, as GSA has done consistently for all its multiple award contract vehicles, such as the IT GWACs, Schedules, and other IDIQ contracts, to determine applicability of regulations and laws.** The proposed plan to allow for each micro-purchase to be a separate contract for purposes of the application of the FAR and statutory requirements is a significant departure from previous GSA acquisition management decisions. It creates parallel contracting programs where in one program certain government requirements apply and another program where they do not. We recommend that GSA, in consultation with OMB, increase transparency by providing the public with a list of requirements that should be eliminated and the rationale as to why their elimination is in the best interest of the Government. This includes the Trade Agreements Act, Buy American Act, and small business preferences, should GSA determine that they should not apply to purchases made through commercial e-marketplace portal(s). Further, if GSA waives these requirements for the proof of concept, the requirements should be waived across GSA's contract portfolio. Finally, we recommend that GSA—
 - a. Consult with the United States Trade Representative regarding any waiver of the Trade Agreements Act and/or Buy American Act for this new \$30 billion contracting program given its significant public and trade policy implications.
3. **Review the standard terms and conditions of commercial e-commerce portal providers in the context of Government requirements as required by Section 846.** To date, the record is devoid of such an assessment. Given that e-marketplace portal provider(s) set the terms and conditions for both third-party suppliers selling on the platform and Federal buyers purchasing on the platform, a thorough review of all such standard terms and conditions is necessary under Section 846. **GSA and OMB's extensive review should include among others:**
 - a. **Price Parity provisions** that limit the discounts/prices third-party suppliers can offer customers via other sites and/or other channels.
 - b. **Pay for Play provisions** where in performing a government contract, e-marketplace providers can charge third-party suppliers fees for higher search results, and other advantages, when Federal customers search for products or place orders.
 - c. **Standard terms and conditions that create conditions of entry into the market.** Here again, GSA should reach out to the FTC to identify, review, and assess the competitive impact on the Federal market.
4. **Mitigate the Organizational Conflicts of Interest (OCI) in the current draft RFP which allows an e-marketplace portal provider to sell both third-party supplier products and its own products,**

while at the same time, setting the business rules and fees that impact the sales of both. As currently outlined in the draft RFP, it is unclear how the Government will prevent pilot awardee(s) from promoting their own products over third-party competitors or what would compel portal providers to exercise objectivity between third-party suppliers. It is critical that the Government establish stringent terms and conditions to ensure that fair and open competition is maintained for Federal purchases made through commercial e-Commerce portals. Any fees that are not restricted should be transparent to Federal buyers like the fees for other government contracts.

5. **Include specific terms and conditions in the draft RFP restricting the use of data, consistent with Section 846, as amended.** Significant questions remain about the use and assumptions drawn from data. For example:
 - a. Use of information formatted for data mining purposes should be clarified to be limited to the Government and stringent enforcement provisions should be established to prevent platform provider use of such data.
 - b. Controls should be established linking any release to the stringent requirements of Section 846, as amended.
 - c. A mechanism should be established to monitor e-marketplace provider compliance with prohibitions on the use of third-party transactional data.
6. **Exclude all products (e.g. IT and healthcare) from the pilot where cyber and supply chain risks to Federal agencies and to veterans have not been addressed.** To date, there is no record of data from GSA and OMB that would confirm that inclusion of certain products in the CPI pilot is appropriate. The supply chain risks from a cybersecurity and patient care perspective for veterans and serving military are significant for certain categories of products, like IT and healthcare supplies. While the draft RFP calls for contractors to employ effective supply chain management processes and controls, threshold requirements are lacking, and enforcement mechanisms are not set forth. As such, the prudent course is to exclude certain products (e.g. IT and healthcare) from the proof of concept until the significant cyber and supply chain security and safety issues are appropriately addressed.
7. **Explain what the “ability to migrate existing agency terms and conditions that agencies might already have with the platform providers” as an important B2B feature means in the Statement of Objectives.** Considering the current number of pilots, does this create a competitive advantage for certain e-marketplace portal providers?
8. **Update the draft RFP so that the proof of concept, again, assesses at least the three commercial e-commerce portal models identified in the Phase I report, is limited to a specific subset of agencies and covers a two-year period.** Coalition members are concerned that a government-wide 5-year \$30 billion CPI is not a proof of concept, but more accurately would be characterized as a significant *program* which would assure the awarded portal provider(s) a degree of lock-in in the Federal market with the benefit of being institutionalized into the Government’s e-Commerce infrastructure and long-term strategy through OMB’s implementation guidance to be issued in Phase III. Therefore, consistent with GSA’s intent to begin with a “limited scope approach,” we recommend that the proof of concept of multiple e-commerce model types be limited to a subset of agencies, specified in the final solicitation, and limited to one year with a one-year option.

The Coalition sincerely appreciates your consideration of the extension request. If there are any questions, please contact me at (202) 331-0975 or rwaldron@thecgp.org.

Sincerely,

A handwritten signature in black ink, appearing to read 'RWaldron', with a long horizontal flourish extending to the right.

Roger Waldron
President

Attachment 1: Comprehensive Member Comments

Attachment 2: DoD Report

Attachment 3: Letter



Commercial Platforms Initiative

Comprehensive Comments

The Coalition for Government Procurement (“the Coalition”) appreciates the opportunity to submit comments on the Draft RFP on the Commercial Platforms Initiative (CPI). Our comprehensive comments, provided on behalf of our members, are the following:

The Draft RFP Does Not Leverage Competition Available in the Commercial Market

Section 846 of the National Defense Authorization Act (NDAA) of Fiscal Year 2018 (Section 846) defined an e-Commerce portal broadly, as “a commercial solution providing for the purchase of commercial products aggregated, distributed, sold, or manufactured via an online portal.” This expansive definition affords the Government the ability/opportunity to access multiple e-Commerce solutions, driving healthy competition **between** various e-Commerce portals/solutions. Competition between solutions minimizes the potential for a dominant provider(s) to serve as the gatekeeper(s) to the Government market, thereby restricting competition and limiting access to innovative commercial products.

In response to Section 846, GSA identified three types of e-Commerce portals/solutions: (1) e-Marketplace; (2) e-Commerce; and (3) e-Procurement. The draft RFP seeks contracts with only the “e-Marketplace” model. By excluding the e-Commerce and e-Procurement models, the draft RFP circumvents the expansiveness of Section 846. This approach unnecessarily limits competition now, and over the long term. Further, by not fully exploring all commercial solutions, GSA has sidestepped the forces of the market, thus isolating the Government market from the benefits of competition.

The draft RFP’s exclusion of all portal/solutions other than the e-Marketplace solution will have long term, negative consequences for competition in the federal market. In the draft solicitation, GSA contemplates a five-year “proof of concept” contract, which includes a one-year base period of performance and four additional one-year options, with an annual addressable market of \$6 billion. To date, however, GSA has not publicly announced whether it plans to include the e-Commerce or e-Procurement models in a similar proof of concept. Consequently, this approach, which eliminates all potential alternative solutions for a contract that could represent upwards of \$30 billion over five years, will result in the pre-selection of a technology winner. Moreover, because the initial proof of concept will also serve as the foundation for future governmentwide guidance, this approach will institutionalize a competitive bias that favors e-Marketplace solutions over all other competitive alternatives.

Recognizing that e-Commerce technologies will influence and be influenced by other contracting activities, the distortion of market forces risks cascading into other commercial procurements,

undermining the commercial contracting process established under statute. As currently set forth, GSA's approach would, under the guise of providing incentives for any e-Marketplace provider to participate in the program, adapt agencies' needs and policies to serve the purposes of the e-Marketplace provider, rather than the other way around. The Government has stated that it must incentivize an e-Marketplace provider to participate in this program. With no competition from other solution providers, an e-Marketplace provider can set its own terms.

The Draft RFP Restricts Competition Between e-Marketplace Providers

Not only does the draft RFP unnecessarily/unduly restrict the competition to the e-Marketplace portal solution, it also restricts competition among e-Marketplace solutions. Pursuant to the draft ordering procedures, agency customers could review and/or shop for products within a single e-Marketplace portal provider without examining any other provider awarded under the proof of concept. Under these circumstances, price comparisons will take place solely at the *supplier* level. This limitation on competition within e-Marketplace solutions serves to the benefit of a dominant e-Marketplace provider, and it creates an additional barrier to entry for new providers. For Coalition members, there are several critical risks inherent in GSA's choice to conduct a proof of concept that focuses on only the e-Marketplace model, including:

- Foreclosing Government access to the dynamic forces of the competitive commercial market.
- Foreclosing Government access to evolving technologies and solutions that otherwise are or will be available in the dynamic commercial market.
- Insulating the e-Marketplace solution from the forces of competition, leaving it with little market pressure to improve its services or lower its fees.
- Exploiting the power of the Government and the funds of the taxpayers to establish and subsidize a third-party market gatekeeper with the freedom to control.

In summary, to achieve the benefits of competition and innovation from the commercial market, the draft solicitation should be revised, consistent with the statutory intent of Section 846, to include all types of commercial e-Commerce solutions as part of the proof of concept. By so doing, GSA and OMB could better assess how commercial e-Commerce solutions could be implemented in a manner that supports mission needs.

The Draft RFP Does Not Address Fundamental Government Requirements

As set forth in both the draft solicitation and the Phase II implementation plan, each Micro-Purchase Threshold (MPT) order would be considered as a separate contract for the purpose of applying the relevant Federal Acquisition Regulation (FAR) and statutory requirements. This is a significant departure from GSA acquisition management decisions regarding repetitive orders under contracting programs. For all its multiple award contract vehicles, IT GWACs, Multiple Award Schedules, and other IDIQ contracts, GSA has looked to the estimated volume at the contract level to determine applicability of regulations and laws. Such a long-standing approach has served customer agencies, industry partners, and the taxpayers in ensuring compliance with important public policy requirements. Surprisingly, GSA has taken a different approach here, resulting in certain fundamental procurement policies, such as the Buy American Act (BAA) and the Trade Agreements Act (TAA), not applying to the transactions contemplated under the draft solicitation.

Pursuant to the FAR, there are no required provisions or clauses for micro-purchases, except for FAR 52.232-39 – Unenforceability of Unauthorized Obligations, and FAR 32.1110 (financing). Notably, this means that neither FAR 52.212-4 or FAR 52.212-5, the commercial item standard clauses, would apply. In addition, the following are also not applicable to purchases below the MPT:

- No competition requirements
- No Organization Conflict of Interests (OCI) requirements or reviews
- No BAA
- No TAA
- No small business preferences or provisions

Considering the potential unintended consequences associated with establishing a new, multi-billion dollar contracting program that would waive a host of fundamental government requirements, it would be beneficial for GSA, in consultation with OMB, to identify the specific requirements that they believe should be eliminated and provide stakeholders with its rationale. This approach would be consistent with the statutory intent of Section 846, which states that:

“[a]ll laws, including laws that set forth policies, procedures, requirements, or restrictions for the procurement of property or services by the Federal Government, apply to the program ...”

Moreover, this approach should be applied to all GSA contracting programs to ensure consistent application of Government requirements across the portfolio. To date, GSA and OMB have been silent on the rationale for waiving these requirements and have instead defaulted to the application of the MPT.

GSA Should Consult with the United States Trade Representative Regarding the Waiver of the TAA & BAA

The Trade Agreements Act (TAA) implements the World Trade Organization Government Procurement Agreement (WTO GPA). Generally, under the WTO GPA, signatory countries, including the United States, have agreed not to engage in discriminatory purchasing practices in government procurement against products from eligible countries (*i.e.* products from signatory countries). Specifically, the TAA limits applicable federal procurements to only American products or products from countries that have agreed to not discriminate against each other’s products, per the WTO GPA or Free Trade Agreements.

From a policy perspective, the purpose of the WTO GPA and the TAA is to promote fair and free treatment of American products in foreign government procurement. As noted on the United States Trade Representative (USTR) website:

“A longstanding objective of U.S. trade policy has been to open new procurement opportunities for U.S. goods, services and suppliers to compete on a level playing field for foreign government procurement. Government procurement typically comprises 10 percent to 15 percent of a country’s GDP.”

Throughout the 1990s, and into the 2000s, the USTR supported GSA's application of the TAA to the MAS program, as it was viewed as supportive of the USTR's efforts to open foreign government procurement to American products.

Notably, the draft solicitation contemplates structuring the proof of concept to limit individual transactions to below the MPT of \$10,000 and states that each order below the MPT is a separate contract rather than utilizing the \$30-billion-dollar addressable value of the proof of concept to determine the applicability of fundamental procurement policies. Under these circumstances, GSA would establish, for the first time, a formal contracting program, the value of which could exceed tens of billions of dollars, where the TAA would be waived. Significantly, this approach would allow an e-Marketplace awardee under the draft solicitation to sell and/or deliver millions of dollars of its own non-TAA products. Under these circumstances, it is difficult to understand how the draft solicitation, which would allow for unrestricted access to non-TAA compliant products, is consistent with the USTR's efforts.

Moreover, because the TAA applies to GSA's Multiple Award (MAS) program, products from eligible countries can be purchased by the Federal government, while products from non-WTO GPA countries are ineligible for such purchase. This disparate treatment highlights a potential impact of the draft RFP. It creates parallel contract universes: a pre-existing commercial item contract universe (e.g. the MAS program, NASA SEWP, and NIH CIO-CS) limited to the purchase of TAA products, and a set of e-Commerce portal contracts where products from the non-TAA countries can be offered and purchased. Accompanying those universes will be separate rules and mechanisms, and their associated costs, to assure compliance with the law (e.g. the assessment and monitoring of substantial transformation).

These two fundamentally inconsistent contracting programs will also have direct impacts on contractor sourcing decisions with the potential to fundamentally alter the Federal procurement market and undermine the USTR's efforts to open markets for American products and services.

The Draft RFP Includes No Review of Standard Terms & Conditions

As noted above, Section 846(f)(1):

"[a]ll laws, including laws that set forth policies, procedures, requirements, or restrictions for the procurement of property or services by the Federal Government, apply to the program..."

Further, Section 846(c)(2)(E), directs GSA and OMB, to include as part of the Phase II, Market Analysis and Consultation:

"a review of standard terms and conditions of commercial e-Commerce portals in the context of Government requirements."

To date, there has been no indication that there has been a review of the standard terms and conditions of commercial e-Commerce portal providers. Indeed, not only is such review absent from the Phase II report, there is also no requirement included in the draft solicitation for offerors to submit their standard terms and conditions as part of their proposals.

Considering that e-Marketplace portal providers set the terms and conditions for both third-party suppliers selling on the platform, as well as customers buying from the platform, a holistic, cross-cutting review of all such standard terms and conditions is appropriate and necessary. Significantly, due to the deeply interconnected transactional relationship between e-Marketplace providers and third-party suppliers, the terms and conditions governing that relationship will directly impact Federal customers of the portal. As such, GSA should consult with the Federal Trade Commission as part of this review, paying particular attention to the following:

Price Parity Provisions

Through price parity provisions, e-Marketplace providers can effectively restrict the ability of third-party sellers to provide customers with better pricing, customer service, and/or quality information through alternative channels. Specifically, these provisions require that the purchase price offered through the e-Marketplace provider be at least as favorable as the most favorable terms upon which the product is offered via other sales channels.

Price parity provisions can be restraints of trade. Such provisions raise significant questions regarding competition, pricing, marketplace entry, and innovation. For example, an emerging, more efficient commercial e-Commerce solution might seek to charge lower transaction fees to its third-party suppliers. Those third-party suppliers subject to price parity provisions, however, would be barred from lowering their prices, and thus passing on the resulting savings to Federal buyers. In the context of Section 846, the potential risk to the Government of a price parity provision implemented by a e-Marketplace portal provider is significant. It could result in the e-Marketplace portal serving as the defacto gate keeper for federal procurement, limiting competition and setting prices government-wide through a price parity provision.

Pay for Play:

The draft solicitation poses questions regarding an offeror's capabilities, including the use of fees in exchange for enhanced product placement, raising significant concerns of a "pay-for-play" dynamic. Specifically, under such a scheme, a third-party seller could pay a fee to the marketplace provider in exchange for better product placement.

Coalition members have raised questions as to whether such a scheme represents a kickback prohibited by the Anti-Kickback Act. At minimum, this arrangement violates the spirit of the Anti-Kickback Act as it creates a dynamic where Government purchasing decisions are influenced by search results that are paid for by third-party suppliers to e-Marketplace providers, rather than price, quality, and delivery terms. In the context of the draft solicitation, a pay for play arrangement places a provider in the position controlling the third-party supplier's effective access to, and subsequent sales volume, in the Federal market.

In addition, to the extent that commercial e-Marketplace providers have standard terms and conditions that establish conditions of entry into the market, GSA's Phase II report and draft solicitation are silent as to whether these have been identified or reviewed for potential impacts on competition and access to the Federal market.

The Draft RFP Does Not Identify, Address, or Mitigate Potential Organizational Conflicts of Interest (OCI)

Although the draft solicitation states that the contracting officer has determined that GSA's proof-of-concept carries the potential for organizational conflicts of interest (OCI), it does not provide any specific details regarding what the potential OCI(s) might be. Concurrently, the draft solicitation, as well as GSA's Phase I and II reports, allow for an e-Marketplace awardee to compete against third-party suppliers that are selling on its platform. Under these circumstances, the e-Marketplace portal provider's role as the manager of the platform conflicts with its role as a seller on the platform, creating an OCI. Specifically, under this arrangement, the e-Marketplace provider sets the terms of entry, establishes the search parameters and presentation features, and prescribes the rules pertaining to the method of fulfillment of subsequent orders.

Moreover, the draft solicitation provides no details regarding how the potential OCI(s) might be addressed, which appears to conflict with the requirements set forth under FAR 9.5. Specifically, pursuant to FAR 9.5, Contracting Officers are responsible for identifying OCIs early in the acquisition process, obtaining appropriate legal and technical assistance, and recommending a course of action to resolve significant OCIs to the head of the contracting activity. Notably, the draft solicitation is silent regarding the mitigation of the potential biased ground rules and impaired objectivity OCIs created when the e-Marketplace portal provider competes against third-party suppliers on its own platform.

Significant questions remain about the use and assumptions drawn from data. For instance, the Draft RFP does not bound the use of information formatted for data mining purposes. At the very least, that activity should be clarified to be limited to the Government, and, in light of the statute, stringent enforcement provisions should be in place to prevent any platform provider from using such data. Along these lines, data releases under the draft RFP have vague controls. Controls should be established linking any release to the stringent requirements of Section 846, as amended.

In addition, although the draft solicitation includes proscriptions against the use of third-party supplier transactional data by e-Marketplace providers, it fails to address or provide mechanism to monitor compliance by e-Marketplace providers. Access to the transactional data creates an unequal access to information OCI, which Congress recognized when it included language specifically prohibiting e-Marketplace providers from using such data for their own competitive purposes. Accordingly, the draft solicitation should include additional oversight/monitoring mechanisms to ensure compliance with the Congressional mandate.

Other Considerations

e-Marketplace Orders versus MAS contracts

The language in the draft RFP regarding the interplay between orders via the e-Marketplace and Multiple Award Schedule (MAS) contracts raises more questions than it answers.

If the language is to assure that orders under the proof of concept's e-marketplace do not create legal obligations vis-a-vis a 3rd party supplier's MAS contract, additional clarity in the contract terms and the law is required. As provided in *Photon Technology International, Inc. v. General Services Administration*, General Services Administration Board of Contract Appeals (GSBCA) No. 14918 (June 23, 1999),

contractors must inform all government ordering agencies, including those not required to use a Schedule contract, that they possess a Schedule contract so agencies can take advantage of Schedule contract benefits. Thus, the benefits of the Schedule will need to be identified and aligned with the proof of concept. If the language is to somehow distinguish the supplier as a contractor and not a subcontractor, it is not clear whether that distinction is effective, especially with the incorporation of FAR clauses to the contrary. Finally, it appears that GSA is providing guidance to e-Marketplace contractors and third-party suppliers that will result in customer agencies paying “open market” prices that are higher than MAS prices.

Requirements Definition

The draft solicitation lacks detailed baseline metrics for many factors, including, but not limited to, user experience, the measurement of cyber and supply chain issues, maximizing the use of third-party suppliers, providing account management capabilities, search filtering, cyber and supply chain risk management, and chain of custody issues relating to healthcare products. Although the draft solicitation calls for contractors to employ effective supply chain risk management processes and controls, threshold requirements are lacking, and specific enforcement measures are not stipulated. Similarly, specific acceptable privacy requirements are not defined and set forth. As such, the prudent course is to exclude information technology and healthcare products for the current implementation, providing additional time to address the significant cyber, supply chain, and safety issues. The recent DoD Inspector General report, titled, “Audit of the DoD’s Management of the Cybersecurity Risks for Government Purchases of Commercial Off-the-Shelf Items,” serves to illustrate this point.

Data Analytics/Cost Comparisons

The draft solicitation appears to rely heavily on data analytics, apparently as a supplement to assessing buyer purchasing compliance. It should be recognized that these analyses are *ex post facto*. Thus, to the extent that a noncompliant purchase takes place, such as the purchase and insertion of malware into government systems, damage will be done prior to the time the government is made aware of it.

The draft solicitation also calls for an analysis comparing any savings associated with the proof of concept against programs, like the Schedules. No metrics for measuring those savings, however, are set forth. Thus, the Government risks releasing false data regarding savings, which will undermine oversight of the proof of concept’s utility. Any analysis of savings must assess the Total Cost of Acquisition (TCA) associated with the programs being compared, that is, all direct and indirect costs of acquisition. Without assessing the TCA, the Government runs the risk of focusing merely on a low or high product price, and not the extra or saved costs associated with the resulting price. It would not be accurate, for instance, to consider the e-Marketplace model a failure simply because studies have been found to be the high-cost alternative to GSA Advantage. The Government should understand the fees, direct and indirect, associated with that model, as well.

AbilityOne

GSA has been an invaluable partner with the AbilityOne program in the supply of AbilityOne products and services that support the employment of more than 45,000 Americans who are blind or have significant disabilities. As GSA looks to increase Federal purchasing through commercial e-Commerce portals, the Coalition recommends that the final solicitation include specific contract language on

contractor use of mandatory sources, in addition to the restrictions on 'essentially the same' items and the indicators that help Federal purchasers easily identify AbilityOne items that are outlined in the Statement of Objectives. Specifically, we request that 52.208-9 Contractor Use of Mandatory Sources of Supply and Services be added to Section C.1., FAR Clauses Applicable to the Contract.

GSA Transaction Fee

It is anticipated that GSA will receive up to 0.75% transaction fee under the program. At the outset, if the proof of concept is creating work and associated cost for GSA, it is unclear why it is being considered "no-cost." The program is being implemented by an outside entity. Notably, GSA receives the 0.75% transaction fee for the Schedule Program due to its work in running the program. Under these circumstances, an accounting of its actual costs associated with implementation would be appropriate. Finally, the fee owed to GSA will be calculated based on transactional data provided by the contractor (presumably, the document is speaking of the e-Marketplace portal contractor). Nowhere, however, are there terms identifying how that fee will be audited and validated.

RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES:

AGING

ARMED SERVICES

COMMERCE, SCIENCE, AND TRANSPORTATION

JUDICIARY

VETERANS' AFFAIRS

United States Senate

WASHINGTON, DC 20510

706 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510

(202) 224-2823
FAX: (202) 224-9673

90 STATE HOUSE SQUARE, TENTH FLOOR
HARTFORD, CT 06103
(860) 258-6940
FAX: (860) 258-6958

915 LAFAYETTE BOULEVARD, SUITE 304
BRIDGEPORT, CT 06604
(203) 330-0598

FAX: (203) 330-0608

<http://blumenthal.senate.gov>

December 19, 2018

The Honorable Makan Delrahim
Assistant Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dear Assistant Attorney General Delrahim:

I am deeply concerned that the price parity provisions in Amazon's contracts with third-party sellers could stifle market competition and artificially inflate prices on consumer goods that millions of Americans are planning to buy this holiday season. I urge you to act quickly to protect American shoppers by opening an investigation into these price parity clauses. European officials took action against these clauses five years ago. American consumers deserve the same protections. U.S. antitrust officials should open their own investigation immediately.

Recent economics research has demonstrated that price parity provisions – also known as most-favored nation clauses – can harm consumers, especially when enforced by large tech platforms with significant market power.¹ Given Amazon's leading position in the U.S. e-commerce market,² it may now possess the degree of market power at which its price parity provisions could raise serious competition concerns. Amazon's price parity provisions limit the discounts that third-party merchants can offer to customers who find their products through any site other than Amazon's online marketplace. With few exceptions, Amazon's contract requires that the purchase price that third-party merchants offer on Amazon is "at least as favorable to Amazon Site users as the most favorable terms upon which a product is offered or sold via" other sales channels.³ In the past, Amazon is reported to have enforced these price parity provisions by

¹ See Jonathan B. Baker & Fiona Scott Morton, *Antitrust Enforcement Against Platform MFNs* 127 YALE L.J. 2176 (2018) <https://www.yalelawjournal.org/feature/antitrust-enforcement-against-platform-mfns>; Andre Boik and Kenneth S. Corts, *The Effects of Platform MFNs on Competition and Entry* 59 J.L. & ECON. 105, 113-29 (2016) <https://www.journals.uchicago.edu/doi/abs/10.1086/686971> (finding that platform most favored nations clauses "typically raise platform fees and retail prices and curtail entry or skew positioning decisions by potential entrants pursuing low-end business models.").

² See Emily Stewart, *Happy Prime Day! Experts Worry Amazon is Building a Dangerous Monopoly* Vox (Jul 17 2018) <https://www.vox.com/2018/7/17/17583070/amazon-prime-day-monopoly-antitrust> (regarding Amazon's market share).

³ See Amazon Services Business Solutions Agreement, S-4 (noting that offers to wholesale purchasers and customers that have opted into membership-based customer loyalty or customer incentive programs are excluded from the price-parity provision).

threatening to remove merchants who violated these contract clauses from their marketplace,⁴ a practice that is rumored to have continued in recent years.⁵

Amazon's price parity provisions may raise prices for consumers both in the short term and in the long run. In the short term, these clauses prohibit third-party merchants who sell on online marketplaces with lower transaction fees from passing on any savings to consumers. For example, if a competitor to Amazon charges lower commission fees to third-party merchants operating on its site, Amazon's price parity provision will prohibit sellers from reducing their prices to reflect the lower cost of selling through Amazon's competitor.⁶ In the long run, these provisions may permit Amazon to steadily raise the transaction fees it charges third-party merchants, secure in the knowledge that sellers will either have to accept the higher fees or charge all its online customers higher prices across all sales channels.⁷

Relatedly, Amazon's price parity provisions may work to block the emergence of more efficient online marketplaces that might offer consumers lower prices on their favorite goods. In order to compete with Amazon and attract third-party sellers to its site, another online marketplace might wish to offer reduced transaction fees to third-party merchants selling through online sales channels. One advantage of this market strategy would be to enable third-party merchants to drop their prices for consumers who visit the site, which should attract additional consumers to the site over time. However, because third-party merchants are barred by Amazon's price parity provision from passing on savings from reduced transactions costs to consumers, Amazon's potential competitors may be hamstrung in their efforts to induce sellers to offer consumers a better price. This lack of competition puts additional upward pressure on prices.

Amazon's price parity provisions have already raised serious antitrust concerns among European regulators. Roughly five years ago, British⁸ and German⁹ antitrust officials opened investigations into Amazon's price parity provisions because they were concerned that these contract clauses violated their national competition laws. For example, German antitrust officials found that, because Amazon offers its own retail products alongside those of third-party merchants, these price parity provisions likely constituted an unlawful horizontal restraint on trade that may have led to higher prices and acted as a barrier to entry for competitors.¹⁰

⁴ *Case Report: Amazon Removes Price Parity Obligation for Retailers on Its Marketplace Platform*, Ref.: B6-46/12, Bundeskartellamt 1 (Dec. 9, 2013) <https://perma.cc/5VGV-Q9QF> ("Compliance with the price parity instructions was regularly monitored and enforced by Amazon from 2012 onwards. Amazon threatened the retailers concerned with measures culminating in the withdrawal of the right to sell on amazon.de.").

⁵ *See Price Parity? Threatened with suspension over Price Parity?* (Feb. 26 2018) <https://sellercentral.amazon.com/forums/t/price-parity-threatened-with-suspension-over-price-parity/389017>

⁶ *Cf.* Baker & Scott Morton, *supra* note 1, at 2181-82.

⁷ *Cf.* Boik and Corts, *supra* note 1, at 107.

⁸ BBC News, *Amazon to Alter Pricing Policy for Traders* (Aug. 29 2013) <https://www.bbc.com/news/business-23881202>.

⁹ *Case Report: Amazon Removes Price Parity Obligation for Retailers on Its Marketplace Platform*, Ref.: B6-46/12, Bundeskartellamt 1 (Dec. 9 2013) <https://perma.cc/5VGV-Q9QF>

¹⁰ *Id.*

In response to British and German regulators' investigations, Amazon promised that it would cease enforcing its price parity provisions against European sellers.¹¹ However, it has continued to enforce them in the United States.¹² Amazon consumers in the United States deserve the same protections as their European counterparts.

Just as Amazon's price parity provisions raised concerns abroad, they should raise legal concerns among antitrust regulators at home. Our courts have already found that price parity provisions can be unlawful restraints of trade. For example, the Second Circuit held in 2015 that, in the context of e-book pricing, Apple's price parity agreement – or what the court called a most-favored nation clause – constituted a violation of Section 1 of the Sherman Act.¹³ Amazon's price parity provisions are particularly concerning because at least one other online marketplace – Walmart, which also owns Jet.com¹⁴ – appears to be using a price parity provision.¹⁵ The use of multiple price parity provisions throughout the e-commerce industry raises concerns that these clauses may collectively work to block competition and raise prices in violation of Section 1 of the Sherman Act.¹⁶

Legal scholars have noted that online tech platforms using price parity provisions may run afoul of the Sherman Act's prohibition on attempts to monopolize.¹⁷ The case for challenging Amazon's price parity provisions under Section 2 of the Sherman Act is particularly strong. That is because Amazon controls nearly half of all U.S. e-commerce,¹⁸ which should allow regulators to easily establish that Amazon has the high market share typically necessary to bring successful litigation under Section 2.¹⁹

In light of the strong economic and legal arguments that Amazon's price parity provisions raise antitrust concerns, I urge you to open an investigation into their effect on the marketplace. This would be in line with past practice. For example, the Department of Justice

¹¹ See BBC News, *supra* note 7.

¹² See Amazon Services Business Solutions Agreement, S-4.

¹³ See e.g., *United States v. Apple Inc.*, 791 F.3d 290 (2d. Cir 2015); Baker & Scott Morton, *supra* note 1, at 2191-92 (discussing the Apple MFN).

¹⁴ Andria Cheng, *Walmart's Jet.com Is Getting A Makeover To Try To Win Over New York's Millennials* Forbes (Sept. 13 2018) <https://www.forbes.com/sites/andriacheng/2018/09/13/walmart-jet-redesign-new-york/>.

¹⁵ See e.g. Zentail, *Price Wars: Multichannel Repricing for Amazon, Walmart Marketplace* (May 2017) <https://insider.zentail.com/price-wars-multichannel-re-pricing-for-amazon-walmart-marketplace/> (stating that Walmart's online marketplace has a price parity rule); Walmart Marketplace Program Retailer Agreement, 8. *Parity Pricing, Special Offers and Promotions* <https://marketplace-apply.walmart.com/resource/1454541787000/SellerAgreementDoc> (containing a price parity provision almost identical to Amazon's); see also Spirit of Jet Marketplace, *Pricing* <https://prodimreports.blob.core.windows.net/policies/policy-revision-4.pdf> (stating that the "Retailer Price of an item (i.e., Item Price + Shipping Price) should be equal to or less than what [third party merchants] sell the item for elsewhere, including, but not limited to, any on-site sales or promotions").

¹⁶ See Baker & Scott Morton, *supra* note 1, at 2180 (noting that a price parity provision can "facilitate coordination" by "discourage[ing] discounting and stabiliz[ing] prices," and citing examples).

¹⁷ See 15 U.S.C. §§ 1, 2; Baker & Scott Morton, *supra* note 1, at 2188-89.

¹⁸ See Emily Stewart, *supra* note 2.

¹⁹ Cf. Baker & Scott Morton, *supra* note 1, at 2196 (noting that 30% market share may be sufficient to establish monopoly power for purposes of a case under Section 2 of the Sherman Act).

has pursued cases against price parity provisions in the health and dental insurance industries.²⁰ Our antitrust officials must be similarly aggressive in protecting competition in the online marketplaces that millions of Americans will be visiting this holiday season.

Thank you for your consideration. Please contact Sam Simon or Adam Bradlow in my office at adam_bradlow@blumenthal.senate.gov with any questions and to provide your response.

Sincerely,



Richard Blumenthal
United States Senate

²⁰ See e.g., *United States v. Blue Cross Blue Shield of Mich.*, 809 F. Supp. 2d 665, 671-76, 679 (E.D. Mich. 2011); *United States v. Delta Dental of R.I.*, 943 F. Supp. 172 (D.R.I. 1996).



INSPECTOR GENERAL

U.S. Department of Defense

July 26, 2019



(U) Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items

~~Classified By: Carol N. Gorman
Derived From: DoD Inspector General Action Memorandum
"Cybersecurity Vulnerabilities Identified During the Audit of the
DoD's Implementation of Cybersecurity Controls for Unmanned
Aerial Vehicle Systems"
Declassify On: 50X1 HUM~~

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE





~~SECRET//NOFORN~~

(U) Results in Brief

(U) Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items

July 26, 2019

(U) Objective

(U) We determined whether the DoD assessed and mitigated cybersecurity risks when purchasing commercial off-the-shelf (COTS) information technology items. Although we primarily focused on Government purchase card (GPC) purchases, we also assessed risks affecting traditional acquisition processes.

(U) Background

(U) The DoD purchases and uses a wide variety of COTS information technology items, such as laptops, software, security cameras, and networking equipment. According to the Federal Acquisition Regulation, a COTS item is a commercial item sold in substantial quantity in the marketplace and offered to the Government in the same form in which it is sold to non-Government customers.

(U) The DoD purchases COTS information technology items through several methods, including the traditional DoD acquisition process and GPCs. The traditional acquisition process is used to purchase COTS information technology items used for DoD programs and large acquisitions, such as weapon systems, aircraft, and command and control systems. COTS information technology items are also purchased through the use of GPCs to make micro-purchases, such as a television or an office printer. Micro-purchases are used for purchasing fixed-price commercial supplies that do not require the cardholder to agree to any terms and conditions other than price and delivery. The GPC program is intended to streamline the small purchase and payment process, minimize paperwork, and simplify the administrative process associated with procuring goods that cost less than the micro-purchase threshold of \$10,000.

(U) Findings

~~(U//FOUO)~~ We determined that the DoD purchased and used COTS information technology items with known cybersecurity risks. Specifically, Army and Air Force GPC holders purchased at least \$32.8 million of COTS information technology items, such as Lenovo computers, Lexmark printers, and GoPro cameras, with known cybersecurity vulnerabilities in FY 2018. In addition, we identified that the [REDACTED]

(U) The DoD purchased and used COTS information technology items with commonly known cybersecurity risks because the DoD did not establish:

- (U) responsibility for an organization or group to develop a strategy to manage the cybersecurity risks of COTS information technology items;
- (U) acquisition policies that proactively address the cybersecurity risks of COTS information technology items;
- (U) an approved products list to prevent unsecure items from being purchased; and
- (U) controls to prevent the purchase of high-risk COTS information technology items with known cybersecurity risks similar to the controls implemented through the use of the national security systems-restricted list.

~~(U//FOUO)~~ As a result, adversaries could exploit known cybersecurity vulnerabilities that exist in COTS items purchased by the DoD. If the DoD continues to purchase and use COTS information technology items without identifying, assessing, and mitigating the known vulnerabilities associated with COTS information technology items, missions critical to national security could be compromised. For example, the Department of State issued a warning in May 2017 against using Hangzhou Hikvision Digital Technology Company and

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

(U) Results in Brief

(U) Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items

(U) Findings (cont'd)

(U//FOUO) Dahua Technology Company video surveillance equipment, citing cyberespionage concerns from China. Despite the inherent risks associated with their use, DoD Components continued to purchase and use these COTS items to monitor installation security until Congress banned the Government from using them in August 2018. In addition, despite reports from the National Security Agency, [REDACTED]

[REDACTED], DoD Components purchased and used the systems to [REDACTED]. Using COTS information technology items, [REDACTED]. [REDACTED]. [REDACTED]. [REDACTED]. [REDACTED].

(U) Recommendations

(U) We recommend that the Secretary of Defense direct an organization or group to develop a risk-based approach to prioritize COTS items for further evaluation, a process to test high-risk COTS items, and a process to prohibit the purchase and use of high-risk COTS items, when necessary, until mitigation strategies can limit the risk to an acceptable level.

(U) In addition, we recommend that the Under Secretary of Defense for Acquisition and Sustainment update or develop and implement:

- (U) DoD acquisition policy to require organizations to review and evaluate cybersecurity risks for high-risk COTS items prior to purchase, regardless of purchase method; and
- (U) GPC program policy and training requirements to include training on common cybersecurity risks for COTS information technology items and the impact of the risks to the mission.

(U) We also recommend that the DoD Chief Information Officer update DoD policy to require an assessment of supply chain risks as a condition for approval to be included on the Unified Capabilities Approved Products List.

(U) Furthermore, we recommend that the Under Secretary of Defense for Acquisition and Sustainment and the DoD Chief Information Officer identify and implement administrative solutions, such as expanding the DoD's implementation of its authority to prohibit DoD Components from purchasing COTS information technology items that support national security systems from specific manufacturers to reduce supply chain risks and, if those solutions are insufficient to address the issues identified in this report, seek legislative authority to expand the national security system-restricted list (list of COTS items prohibited from being used in national security systems) DoD-wide to include high-risk COTS information technology items used for non-national security systems.

(U) Management Comments and Our Response

(U//FOUO) [REDACTED]
[REDACTED]
[REDACTED].

(U//FOUO) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

(U) Results in Brief

(U) Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items

(U) Management Comments (cont'd)

(U//FOUO) [REDACTED]

[REDACTED].¹

(U//FOUO) However, comments from the Under Secretary and Chief Information Officer did not address the specifics of the recommendation to develop a risk-based approach to prioritize COTS items for further evaluation, a process to test high-risk COTS items, and a process to prohibit the purchase and use of high-risk COTS items, when necessary, until mitigation strategies can limit the risk to an acceptable level. Responsibility for identifying, testing, and mitigating cybersecurity risks is decentralized among many organizations with overlapping responsibilities and the risk identification processes are not effective at identifying high-risk COTS items that are used DoD-wide and ensuring that all high-risk COTS items are tested. In addition, [REDACTED]

[REDACTED]. Therefore, the recommendations are unresolved and the Acting Secretary of Defense, Under Secretary of Defense for Acquisition and Sustainment, or DoD Chief Information Officer, should provide additional comments identifying specific actions to address the recommendation.

(U) The Under Secretary of Defense for Acquisition and Sustainment agreed with the recommendations to update DoD acquisition policy and GPC policy and training requirements, stating that she will update DoD acquisition policy and GPC program policy and training. In addition, the DoD Chief Information Officer agreed with the recommendation to update DoD policy to require an assessment of supply chain risks as a condition for approval to be included on the Unified Capabilities Approved Products List.

(U//FOUO) The Under Secretary of Defense for Acquisition and Sustainment and DoD Chief Information Officer agreed with the intended outcome of the recommendation to expand legal authorities to include high-risk COTS information technology items used for non-national security systems. However, they stated that [REDACTED]

[REDACTED]

(U) Please see the Recommendations Table on the next page for the status of the recommendations.

¹ (U) Public Law 115-390, "The Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act," December 21, 2018 and Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019.

~~SECRET//NOFORN~~

(U) Recommendations Table

Unclassified Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Secretary of Defense	1.a, 1.b, 1.c	None	None
Under Secretary of Defense for Acquisitions and Sustainment	None	2.a, 2.b	4
DoD Chief Information Officer	None	3	4 Unclassified

(U) Please provide Management Comments by August 26, 2019.

(U) The following categories are used to describe agency management's comments to individual recommendations:

- **(U) Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **(U) Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **(U) Closed** – OIG verified that the agreed upon corrective actions were implemented.





INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

July 26, 2019

MEMORANDUM FOR SECRETARY OF DEFENSE
UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND
SUSTAINMENT
DOD CHIEF INFORMATION OFFICER

SUBJECT: Audit of the DoD's Management of the Cybersecurity Risks for
Government Purchase Card Purchases of Commercial Off-the-Shelf
Items (Report No. DODIG-2019-106)

(U) This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) This report contains three recommendations that are considered unresolved because management officials did not fully address the recommendations. Therefore, as discussed in the Recommendations, Management Comments, and Our Response sections of this report, the recommendations will remain open. We will track these recommendations until an agreement is reached on the actions to be taken to address the recommendations. Once an agreement is reached, the recommendations will be considered resolved but will remain open until adequate documentation has been submitted showing that the agreed-upon action has been completed. Once we verify that the action is complete, the recommendations will be closed.

(U) This report also contains three recommendations that are considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations may be closed when we receive adequate documentation showing that all agreed-upon actions have been completed. Once we verify that the action is complete, the recommendations will be closed.

(U) DoD Instruction 7650.03 requires that all recommendations be resolved promptly. For the unresolved recommendations, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. For the resolved recommendations, please provide us within 90 days your response concerning specific actions in process or completed on the recommendations.

(U) Your response should be sent as a PDF file to [REDACTED] and [REDACTED]. Responses must have the actual signature of the authorizing official for your organization.

(U) We appreciate the cooperation and assistance received during the audit. Please direct questions to me at (703) 699-7331 (DSN 499-7331).



Carol Gorman
Assistant Inspector General for Audit
Cyberspace Operations

(U) Contents

(U) Introduction.....	1
(U) Objective.....	1
(U) Background	1
(U) Review of Internal Controls.....	4
(U) Finding.....	5
(U) Improved Cybersecurity Risk Management Needed for Purchases of COTS Information Technology Items.....	5
(U) The DoD Purchased and Used COTS Information Technology Items With Known Cybersecurity Risks	6
(U) The DoD Did Not Develop Controls to Prevent the Purchase of COTS Information Technology Items With Cybersecurity Risks.....	9
(U) Using COTS Items With Cybersecurity Risks Weakens National Security.....	17
(U) Recommendations, Management Comments, and Our Response.....	19
(U) Appendix A	25
(U) Scope and Methodology	25
(U) Use of Computer-Processed Data	27
(U) Prior Coverage	28
(U) Appendix B	29
(U//FOUO) [REDACTED]	29
(U) Appendix C	35
(U//FOUO) [REDACTED]	35
(U) Appendix D	40
(U) Banned or Restricted COTS Items and Manufacturers.....	40
(U) Management Comments.....	42
(U) Acting Secretary of Defense.....	42
(U) Under Secretary of Defense for Acquisitions and Sustainment and DoD Chief Information Officer	43
(U) Acronyms and Abbreviations	47
(U) Glossary.....	48
(U) Annex: Classified Sources	50

(U) Introduction

(U) Objective

(U) We determined whether the DoD assessed and mitigated cybersecurity risks when purchasing commercial off-the-shelf (COTS) information technology items.

(U) Background

(U) The DoD purchases and uses a wide variety of COTS information technology items, such as laptops, software, cameras, and networking equipment. According to the Federal Acquisition Regulation, a COTS item is a commercial item sold in substantial quantity in the marketplace and offered to the Government in the same form in which it is sold to non-Government customers.² Some COTS information technology items can be used as embedded components in command and control; communications; and intelligence, surveillance, and reconnaissance systems. In July 2018, the Deputy Director, Cybersecurity Risk Management, DoD Chief Information Officer (CIO), estimated that 70 to 80 percent of the components that comprise DoD systems are COTS items.

(U) The DoD purchases COTS information technology items through several methods, including traditional DoD acquisition process and GPCs. The traditional acquisition process is used for COTS information technology items purchased and used in DoD programs and large acquisitions, such as weapon systems, aircraft, and command and control systems. COTS information technology items are also purchased with a GPC to make micro-purchases, such as a television or an office printer.³ The GPC Program is intended to streamline the process to make and pay for small purchases, minimize paperwork, and generally simplify the administrative process associated with procuring goods under the micro-purchase threshold. Although we primarily focused on GPC purchases, we also assessed risks affecting traditional acquisition processes.

² (U) Federal Acquisition Regulation Part 2 “Definitions of Words and Terms,” Subpart 2.1 “Definitions.”

³ (U) Micro-purchases are purchases made for fixed-price commercial supplies and services that do not require the cardholder to agree to any terms and conditions other than price and delivery. These purchases are limited to the applicable micro-purchase threshold. The FY 1998 National Defense Authorization Act mandated the use of the streamlined micro-purchase procedures for at least 90 percent of micro-purchases. This commonly entails the use of GPCs.

(U) DoD Instruction 5000.02 requires DoD Components to implement controls to manage cybersecurity risks throughout an acquisition program's life cycle.⁴ DoD Components must also comply with DoD Instruction 8500.01, which requires DoD Components to implement a cybersecurity program to manage risk for information technology systems or components based on the importance of supported missions and the affected information or assets.⁵ The Instruction also states that DoD agencies must manage, mitigate, and monitor risks associated with global sourcing and distribution.

(U) The DoD's Increased Reliance on COTS Information Technology Items

(U) Since the 1990s, Federal and DoD policy has streamlined the acquisition process to make it easier to purchase COTS items, including COTS information technology items. The Federal Acquisition Streamlining Act of 1994 established a preference for procuring COTS items over those specifically developed for Government use.⁶ More recently, a June 2018 memorandum exempted DoD personnel from complying with certain acquisition regulations when purchasing innovative COTS items, technologies, or services.⁷ Furthermore, between July 2017 and August 2018, the DoD and Congress increased the maximum threshold for a single GPC micro-purchase from \$3,500 to between \$5,000 and \$10,000.⁸ As it has become easier to purchase COTS items, DoD systems have become increasingly reliant on COTS information technology items due to their high utility, low cost, and ease of deployment.

(U) The DoD also continues to increase its use of Internet-connected COTS items. Devices that have the ability to connect to the Internet with a unique Internet Protocol address and can transfer data over a network without requiring human-to-human or human-to-computer interaction are commonly referred to as internet of things (IoT) devices. The DoD uses IoT devices to support missions and operations; for example, the fully networked F-35 Joint Strike Fighter uses IoT-connected devices to collect data to improve the pilot's situational awareness. In addition, the DoD uses thousands of network-connected sensors in its facilities to improve energy efficiency.

⁴ (U) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," August 10, 2017, (Incorporating Change 3).

⁵ (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014. DoD information technology includes any information technology that receives, processes, stores, displays, or transmits DoD information.

⁶ (U) Public Law 103-355, "Federal Acquisition Streamlining Act of 1994," October 13, 1994.

⁷ (U) Under Secretary of Defense for Acquisition and Sustainment Memorandum, "Class Deviation-Defense Commercial Solutions Opening Pilot Program," June 26, 2018, exempts DoD personnel from submitting a summary of a proposed contract and promoting competition.

⁸ (U) Under Secretary of Defense for Acquisition and Sustainment Memorandum, "Class Deviation-Micro-Purchase Threshold, Simplified Acquisition Threshold, and Special Emergency Authority," April 13, 2018, and Public Law 115-232, "National Defense Authorization Act for FY 2019," Title VII, Subtitle B, Section 821, August 13, 2018.

(U) COTS Information Technology Items Are Increasingly Vulnerable

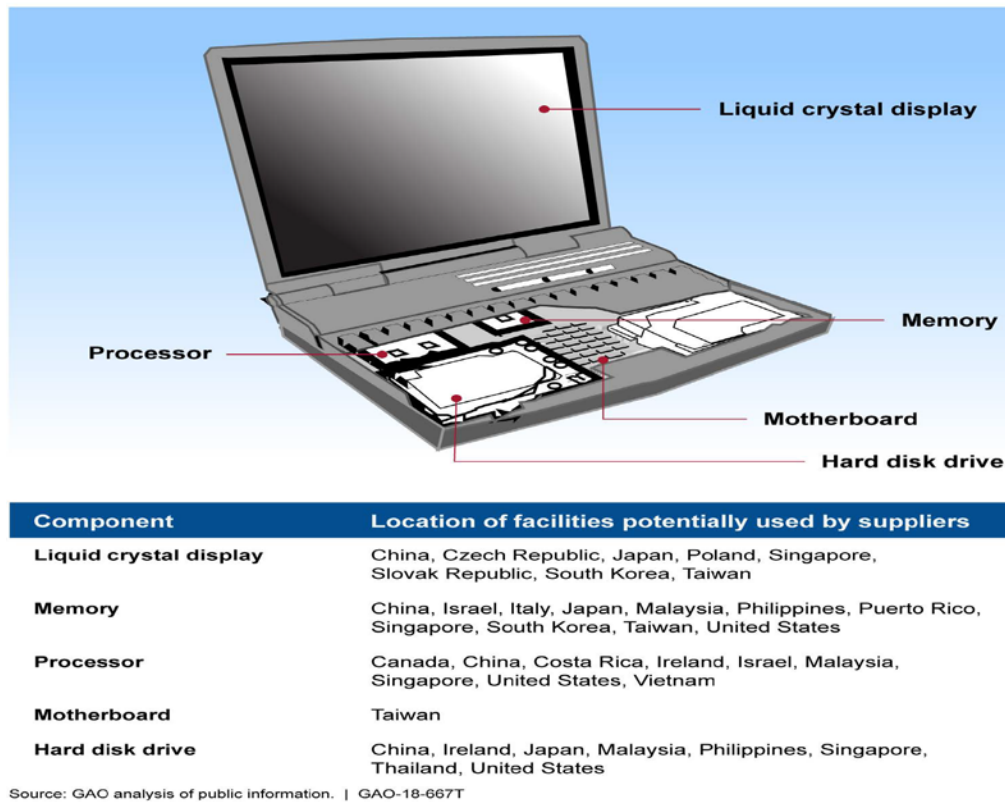
(U) Federal agencies have reported cybersecurity risks associated with using COTS information technology items, such as:

- (U) third-party service providers and manufacturers with physical or logical access to sensitive Government information systems, software code, or intellectual property;
- (U) poor personnel information security practices, such as using applications on mobile devices that provide the location of troops or ongoing DoD operations;
- (U) counterfeit software or hardware with embedded malware, such as viruses or malicious code, that could allow adversaries remote access to DoD systems and networks; and
- (U) a contractor's inability to protect data and mitigate vulnerabilities on systems and networks that store and transmit sensitive information.

(U) Components of COTS information technology items, such as hardware, firmware, and software, can come from globally distributed supply chains that are complex and limit the purchaser's understanding and control over how the components of COTS information technology items are developed, integrated, and deployed. The supply chain is the activities associated with providing materiel from a raw stage to an end user as a finished product. According to the Committee on National Security Systems, adversaries and malicious actors use the supply chain to introduce cybersecurity vulnerabilities into DoD weapon systems and information technology networks that use COTS information technology products.⁹ For example, Figure 1 illustrates an example of potential countries that commonly provide various components in building commercially available laptops.

⁹ (U) Committee on National Security Systems Directive 505, "Supply Chain Risk Management," July 26, 2017.

(U) Figure 1. Potential Origins of Common Suppliers of Laptop Components



(U) Review of Internal Controls

(U) DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.¹⁰ We identified internal control weaknesses with how the DoD identifies, assesses, and manages the cybersecurity risks associated with COTS items, and how the DoD ensures that its personnel are aware of known cybersecurity or supply chain risks when purchasing and using COTS items. We will provide a copy of the report to the senior official responsible for internal controls in the Offices of the Secretary of Defense, Under Secretary of Defense for Acquisition and Sustainment (USD[A&S]), and DoD CIO.

¹⁰ (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

(U) Finding

(U) Improved Cybersecurity Risk Management Needed for Purchases of COTS Information Technology Items

(U//FOUO) The DoD purchased and used COTS information technology items with known cybersecurity risks. Specifically, Army and Air Force GPC holders purchased at least \$32.8 million of COTS information technology items, such as Lenovo computers, Lexmark printers, and GoPro cameras, with known cybersecurity vulnerabilities in FY 2018.¹¹ In addition, we identified [REDACTED]. The DoD purchased and used COTS information technology items with commonly known cybersecurity risks because the DoD did not establish:

- (U) responsibility for an organization or group to develop a strategy to manage the cybersecurity risks of COTS information technology items;
- (U) acquisition policies that proactively address the cybersecurity risks of COTS information technology items;
- (U) an approved products list (APL) to prevent unsecure items from being purchased; and
- (U) controls to prevent the purchase of high-risk COTS information technology items with known cybersecurity risks similar to the controls implemented through the use of the national security systems-restricted list.

(U//FOUO) As a result, the DoD increased its risk that adversaries could exploit known cybersecurity risks. If the DoD continues to purchase and use COTS items without identifying, assessing, and mitigating known vulnerabilities associated with COTS items, missions critical to national security could be compromised. For example, the Department of State issued a warning in May 2017 against using Hangzhou Hikvision Digital Technology Company and Dahua Technology Company video surveillance equipment, citing cyberespionage concerns from China. Despite the inherent risks associated with their use, DoD Components continued to purchase and use these COTS items to [REDACTED] until Congress

¹¹ (U) The Navy did not track COTS item purchases using an enterprise-wide database, instead, the Navy managed the process manually. Therefore, we did not include Navy COTS item purchases in our audit scope.

(U//FOUO) banned the Federal Government from using them in August 2018. In addition, despite reports from [REDACTED]

[REDACTED], DoD Components purchased and used the systems. Using COTS information technology items, [REDACTED]

(U) The DoD Purchased and Used COTS Information Technology Items With Known Cybersecurity Risks

(U//FOUO) The DoD purchased and used COTS information technology items with known cybersecurity risks. In addition, [REDACTED] and issued a notice of concern to the Secretary of Defense.

(U) FY 2018 Purchases of COTS Information Technology Items With Cybersecurity Risks

(U) We reviewed purchases of COTS information technology items for the Army and Air Force and determined that GPC holders purchased at least \$32.8 million of COTS information technology items with known cybersecurity risks in FY 2018.¹² Known cybersecurity risks are included in the National Vulnerabilities Database, or derived from congressional reports, DoD reports, and open source test reports. For example, Army and Air Force GPC holders purchased over 8,000 Lexmark printers, totaling more than \$30 million, for use on Army and Air Force networks. According to a Congressional report on supply chain vulnerabilities from China, Lexmark is a company with connections to Chinese military, nuclear, and cyberespionage programs.¹³ The National Vulnerabilities Database lists 20 cybersecurity vulnerabilities for Lexmark, including storing and transmitting sensitive network access credentials in plain text and

¹² (U) We obtained GPC purchase data from Army's Computer Hardware, Enterprise Software, and Solutions contracts and the Air Force's Network-Centric Solutions-2 Products and Information Technology Commodity Council contracts to identify COTS information technology items purchased by Army and Air Force GPC holders. We could not determine the total value of Army GPC purchases because of the ability to bypass the system to make purchases, or Air Force GPC purchases because of the decentralized tracking of COTS purchases and inadequate system reporting.

¹³ (U) U.S.-China Economic and Security Review Commission Report, "Supply Chain Vulnerabilities From China in U.S. Federal Information and Communications Technology," April 2018.

(U) allowing the execution of malicious code on the printer.¹⁴ These vulnerabilities could allow remote attackers to use a connected Lexmark printer to conduct cyberespionage or launch a denial of service attack on a DoD network. In another example, the Army and Air Force purchased 117 GoPro action cameras at a cost of just under \$98,000. GoPro cameras are designed to film and share video in real-time through a wireless network or Bluetooth connection. However, the cameras have vulnerabilities that could allow a remote attacker access to the stored network credentials and live video streams. By exploiting these vulnerabilities, a malicious actor could view the video stream, start recording, or take pictures without the user's knowledge.

(U) Although the Navy purchased COTS information technology items using GPCs, it did not track the purchases using an enterprise-wide database. Without tasking specific Navy commands to compile the information manually, we could not assess the number or value of COTS item purchases for the specific items we identified with known vulnerabilities. For example, Lexmark printers are available for purchase through the Navy Marine Corps Intranet COTS Catalog and have been certified for use on the Navy network as recently as February 2019.

(U) In addition, the DoD has not banned the purchase and use of Lenovo products despite known cybersecurity risks. Lenovo is the largest computer company in China. Congress and the Department of Homeland Security, among other Government agencies, have issued multiple warnings about the cybersecurity risks of using Lenovo products. In 2006, the State Department banned the use of Lenovo computers on their classified networks after reports that Lenovo computers were manufactured with hidden hardware or software used for cyberespionage. In 2015, the Department of Homeland Security issued cybersecurity warnings related to pre-installed spyware and other cybersecurity vulnerabilities identified in Lenovo computers. In 2016, the Joint Chiefs of Staff Intelligence Directorate issued a warning that Lenovo computers and handheld devices could introduce compromised hardware into the DoD supply chain, posing a cyberespionage risk to classified and unclassified DoD networks. In 2018, 12 years after the State Department ban, the DoD ordered an operational risk assessment of Lenovo products throughout the DoD Information Network to identify and understand the risks Lenovo products posed to the network. In the meantime, the Army purchased another 195 Lenovo products, totaling just under \$268,000, and the Air Force purchased 1,378 Lenovo products for \$1.9 million in FY 2018. The Navy did not offer any Lenovo products on its Certified Device List or COTS Catalog.

¹⁴ (U) The National Vulnerabilities Database is the U.S. Government repository of cybersecurity vulnerability management data including security-related software flaws, misconfigurations, product names, and impact metrics. The database is maintained by the National Institute of Standards and Technology.

(U//FOUO)

(S//NF)

. On May 14, 2018, we issued a notice of concern to the Secretary of Defense, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]. (See Appendix B for the May 2018 notice of concern and Appendix C for the Deputy Secretary of Defense, DoD CIO, and USD(A&S) responses and a description of their corrective actions.) We identified the risk that [REDACTED]



[REDACTED]
[REDACTED]
[REDACTED]. For example, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED], but did not take action to reduce those risks until we issued the notice of concern in May 2018.

(S//NF) In the notice of concern, we also identified problems with how the Military Services managed [REDACTED]. We determined that the Military Services did not have procedures for [REDACTED].

Despite the [REDACTED]
[REDACTED], the DoD did not take steps to [REDACTED]
[REDACTED]. This occurred because [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]. We suggested that the Secretary of Defense issue a [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

(S//NF) On May 23, 2018, the Deputy Secretary of Defense [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. Actions taken by the Deputy Secretary of Defense, USD(A&S),
and DoD CIO addressed all specifics of the suggested actions identified in the notice
of concern related to [REDACTED]
[REDACTED]
[REDACTED].

(U) The DoD Did Not Develop Controls to Prevent the Purchase of COTS Information Technology Items With Cybersecurity Risks

(U) The DoD purchased and used COTS information technology items with commonly known cybersecurity risks because the DoD did not establish:

- (U) responsibility for an organization or group to develop a strategy to manage the cybersecurity risks of COTS information technology items;
- (U) acquisition policies that proactively addressed the cybersecurity risks of COTS information technology items;
- (U) an APL to prevent unsecure items from being purchased; and
- (U) controls to prevent the purchase of high-risk COTS information technology items with known cybersecurity risks similar to the controls implemented through the use of the national security systems-restricted list.

(U) The DoD Did Not Have an Organization Responsible for Managing the Cybersecurity Risks of COTS Information Technology Items

(U) The DoD did not establish responsibility for an organization or group for managing the cybersecurity risks posed by COTS information technology items across the DoD. We reviewed DoD acquisition policy and the items banned from purchase or use by Congress and the DoD and did not identify an organization responsible for managing the cybersecurity risks of COTS information technology items. Specifically, DoD Instruction 5000.02 requires risks to be managed by DoD Components and program offices; but does not require management of the risks at a DoD-wide level.

(U) However, each of these organizations' responsibilities is limited in scope; therefore, a strategic risk-based approach for managing the cybersecurity risks of COTS information technology items was not implemented. We identified the following organizations that only addressed the cybersecurity risks of COTS information technology for specific uses within the DoD.

- (U) The Office of the Under Secretary of Defense for Research and Engineering Joint Federated Assurance Center is responsible for evaluating hardware and software—including COTS hardware and software—for cybersecurity vulnerabilities at the request of a specific program office. The Assurance Center was established in February 2015, but has yet to achieve full operational capability. However, even after the Assurance Center achieves full operational capability, DoD Components are not currently required to submit to the Assurance Center the products that need testing, use Assurance Center-approved products, or follow the Assurance Center's recommendations. In addition, the Assurance Center is not required to share vulnerabilities identified with other organizations.
- ~~(U//FOUO)~~ The Defense Intelligence Agency Supply Chain Risk Management Threat Assessment Center is responsible [REDACTED]. However, according to the FY 2018 National Defense Authorization Act (NDAA), the Assessment Center's threat assessments should [REDACTED]. Requests for reports on COTS information technology items used in [REDACTED] and, according to the DoD CIO Deputy Director for Cybersecurity Risk Management, [REDACTED]

(U//FOUO) [REDACTED]

[REDACTED] for analysis it receives each year. The analysis, however, is classified and most GPC holders cannot access the information due to clearance limitations and are otherwise unaware of the analysis reports.

- (U) The National Information Assurance Partnership is responsible for overseeing the evaluations of COTS information technology for national security systems (NSS).¹⁵ Any COTS information technology item that will be used in an NSS must first meet the strict cybersecurity criteria and testing standards set by the National Information Assurance Partnership. The National Information Assurance Partnership's Product Compliant list is publicly available; however, the list primarily consists of COTS information technology networking equipment and software, and project managers for non-NSS programs are not obligated to purchase from the list.

(U) Although the assessments and analysis completed by DoD organizations are essential to identifying cybersecurity risks for select COTS information technology items, the assessments do not address the impact of using the items DoD-wide and do not consider the risks associated with their use in different operational environments. When purchasing a UAS for command use, a commander is primarily concerned with the risk to his command and mission. When multiple commands use the same type of UAS for various missions, the risk expands exponentially and may become unacceptable when viewed from a DoD-wide perspective. An organization or group responsible for identifying COTS items with cybersecurity risks would help the DoD manage the cybersecurity risks of COTS items, including supply chain and counter-intelligence risks, known from all available intelligence sources, such as industry sources, independent testing, military laboratory testing, and intelligence reports. The Secretary of Defense should direct an organization or group to develop a risk-based approach to prioritize COTS items for further evaluation; a process to test high-risk COTS items; and a process to prohibit the purchase and use of COTS items, when necessary, until mitigation strategies can limit the risk to an acceptable level.

¹⁵ (U) Section 3552, title 44, United States Code, 2014, defines NSSs as information systems that are classified in the interest of national defense, foreign policy, or support intelligence activities critical to meeting military or intelligence missions; cryptologic activities related to national security; command and control of military forces; or equipment that is integral to a weapon system.

(U) DoD Policies Were Insufficient to Proactively Address Cybersecurity Risks for COTS Information Technology Items

(U) DoD policies did not proactively address the cybersecurity risks of COTS information technology items. DoD acquisition policy did not consider the cybersecurity risks of COTS information technology items prior to their acquisition and integration into DoD programs. Similarly, GPC policy does not require acquisition officers or cardholders to consider the cybersecurity risks of COTS information technology items prior to purchase and use.

(U) DoD Acquisition Policy Did Not Address Cybersecurity Risks of COTS Information Technology Items Prior to Purchase and Use

(U) DoD acquisition policy did not require DoD Components to consider known cybersecurity risks before acquiring COTS information technology items or to mitigate cybersecurity risks before integrating the items into DoD programs. The USD(A&S) issued DoD Directive 5000.01 and DoD Instruction 5000.02 to manage the acquisition process; however, the requirements for cybersecurity focus on large programs, such as weapon systems; command, control, communications, and computers; intelligence, surveillance, and reconnaissance systems; and information technology systems. In addition, DoD policy focuses on mitigating cybersecurity risks after purchase.¹⁶

(U) DoD policy focuses on identifying and mitigating cybersecurity risks affecting whole systems instead of the risks associated with the individual COTS information technology items.

For example, DoD Instruction 5000.02 requires acquisition managers to implement controls to address cybersecurity risks through the Risk Management Framework process; however, the process addresses cybersecurity risks after COTS information technology items are acquired and integrated in a program.¹⁷ The DoD CIO Deputy Director for Cybersecurity Risk Management

stated that DoD policy focuses on identifying and mitigating cybersecurity risks affecting whole systems instead of the risks associated with the individual COTS information technology items that make up the system.

¹⁶ (U) DoD Directive 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, (Incorporating Change 3, August 10, 2017).

¹⁷ (U) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, (Incorporating Change 2, July 28, 2017).

(U) The DoD's increased reliance on COTS information technology items as components for larger systems increases the risk that missions and operations could be compromised by adversaries who exploit known cybersecurity vulnerabilities. Assessing overall systems without assessing each component masks vulnerabilities and limits the DoD's ability to identify cybersecurity risks and implement mitigating solutions. The DoD needs to adapt its acquisition processes and ensure that DoD policy aligns with the need to proactively assess and mitigate cybersecurity risks associated with its increased use of COTS information technology items. The USD(A&S) should update existing DoD acquisition policies or develop and implement new policy to require organizations to review and evaluate cybersecurity risks, including supply chain and counterintelligence risks, for high-risk COTS items prior to purchase, regardless of purchase method.

(U) GPC Policy and Training Did Not Address Cybersecurity Risks of COTS Information Technology Items

(U) DoD acquisition policy also did not require GPC acquisition officers or cardholders to consider cybersecurity risks before making a purchase, or prohibit GPC purchases of items with known cybersecurity risks. DoD GPC policy requires DoD Components to establish internal controls to prevent misuse of GPCs and GPC holders to complete initial and refresher GPC training.¹⁸ GPC acquisition officers and cardholders have the discretion and authority to purchase COTS information technology items up to \$10,000. However, according to the DoD CIO's Deputy Director of Cybersecurity Risk Management, acquisition officers and cardholders are generally unaware of potential cybersecurity risks COTS information technology items could have to DoD missions and operations. For example, GPC holders often do not have the security clearance to access DoD reports related to known cybersecurity risks of COTS information technology items, nor are they instructed, trained, or required to research unclassified cybersecurity risks of COTS information technology items before purchase.

¹⁸ (U) USD(A&S), Defense Pricing & Contracting, "Department of Defense Government Charge Card Guidebook for Establishing and Managing Purchase, Travel, and Fuel Card Programs," October 1, 2017 (updated January 24, 2018). DoD GPC training primarily focuses on using the GPCs responsibly and for authorized purposes.

(U//FOUO) Additionally, GPC holders are subject to the orders of their commanding acquisition officers, who may not understand the cybersecurity risks of COTS information technology items. For example, the DoD CIO identified that [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

According to the DoD CIO Deputy Director for Cybersecurity Risk Management, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED].

(U//FOUO) [REDACTED]
[REDACTED]
[REDACTED].

[REDACTED]. GPC acquisition officers and cardholders could provide the first defense to reduce the risk of purchasing and using COTS information technology items with known cybersecurity risks. However, without appropriate training, GPC acquisition officers and cardholders are not prepared to evaluate a COTS item's cybersecurity risk before purchasing. The USD(A&S) should update GPC program policy and training to include training on common cybersecurity risks, including supply chain and counterintelligence risks, for COTS information technology items and the impact of the risks to the mission.

(U) The DoD's APL Is Limited in Scope and Includes COTS Information Technology Items With Cybersecurity Risks

(U) The DoD's APL included COTS information technology items with known cybersecurity risks. An APL is a consolidated list of networking products approved by the Defense Information Systems Agency after the completion of independent laboratory testing that are meant to ensure the security of COTS information technology products used on DoD information systems. DoD Instruction 8100.04 requires the Defense Information Systems Agency to develop and maintain the Unified Capabilities APL and ensure that the products on the list meet technical interoperability and cybersecurity requirements.¹⁹ The DoD uses an APL to support purchasers, including GPC holders, as they make decisions to purchase COTS information technology items that will connect to DoD systems and networks. COTS information technology items included on the DoD Unified Capabilities APL are subsequently included in the Military Services' enterprise buying programs that GPC holders use to purchase approved COTS information technology items.

¹⁹ (U) DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010.

(U) However, the Unified Capabilities APL includes COTS information technology items with known cybersecurity risks. For example, the APL includes Lenovo products which have known cybersecurity vulnerabilities. According to the Chief of the Assessments and Authorizations Division at the Defense Information Systems Agency, cybersecurity risks introduced through the supply chain are not considered when evaluating whether to add COTS information technology items to the DoD Unified Capabilities APL. The DoD CIO Deputy Director for Cybersecurity Risk Management acknowledged that DoD acquisition policy, including GPC purchase and APL testing requirements, has not been updated to reflect the growing cybersecurity and supply chain risks, thereby limiting the policy's usefulness and effectiveness in preventing COTS information technology items with cybersecurity risks from being included on the APL and used on DoD networks. The DoD CIO should revise DoD Instruction 8100.04 to require an assessment of supply chain risks as a condition for approval to be included on the Unified Capabilities APL.

(U) The DoD Did Not Establish Controls to Prevent the Purchase of COTS Information Technology Items With Known Cybersecurity Risks

(U) The DoD did not establish controls to prevent the purchase and use of COTS information technology items with known cybersecurity risks. We identified nine COTS information technology items purchased and used by the DoD that Congress, the DoD, or other Federal agencies later banned because of cybersecurity risks. However, we did not identify any purchases of these nine COTS information technology items once the bans occurred. The organizations banned COTS information technology items such as hardware, software, services and video surveillance equipment because of risks associated with cyberespionage; unauthorized system or network access; and foreign government ownership, control, or influence. The DoD also banned other COTS items, such as fitness trackers, that use geolocation-capable applications because of the cybersecurity risks posed to missions and operations. (See Appendix D for a history of COTS items with banned or restricted use related to cybersecurity or supply chain risks.) The following are examples that highlight the slow process to develop a ban for COTS information technology items and manufacturers.

- (U) The House Permanent Select Committee on Intelligence issued a report in 2012 recommending that U.S. Government systems and Government contractors not use Huawei or ZTE telecommunications equipment or component parts in their systems, especially sensitive systems. The report stated that malicious Chinese hardware or software implants would be a “potent

(U) espionage tool for penetrating sensitive U.S. national security systems.” Despite this report, the DoD did not take action to ban the use of Huawei or ZTE products. In 2017, Congress took action and prohibited the DoD from procuring any telecommunications equipment from Huawei or ZTE.

- (U) The Central Intelligence Agency was aware of the cybersecurity risks of Kaspersky Lab products as early as 2013, suspecting that Kaspersky Lab was a tool of the Russian government. In 2015, according to New York Times and Washington Post reports, Israeli intelligence officials notified the National Security Agency that Russian hackers were searching for and retrieving U.S. intelligence secrets by exploiting the Kaspersky Lab software installed on computers. According to the Wall Street Journal, in 2016, the National Security Agency discovered that Russian hackers used vulnerabilities within Kaspersky Lab software to steal highly classified NSA materials. Despite these reports, the DoD did not ban the use of Kaspersky Lab products. In 2017, Congress banned all Federal departments and agencies from using hardware, software, and services from Kaspersky Lab. Many computer hardware manufacturers have partnered with Kaspersky Lab to embed Kaspersky’s cybersecurity software code into their firewalls, routers, and servers, making it difficult to detect.

(U) Of the nine COTS information technology manufacturers or items that have been banned, four were banned by Congress instead of the DoD despite numerous reports of cybersecurity vulnerabilities. In addition, it took Congress approximately 5 years to

(U) The DoD banned these items in response to cybersecurity incidents or public exposure, not based on risks identified through a process.

ban two items after the cybersecurity risks were known. The DoD banned four of the nine items and issued a warning against purchase for a fifth item; however, the DoD banned these items in response to cybersecurity incidents or public exposure, not based on risks identified through a process to assess COTS information technology items for cybersecurity risks. The Secretaries of

Defense, Army, Navy, and Air Force have the authority to prohibit DoD Components from purchasing COTS information technology items that support NSSs from specific manufacturers to reduce supply chain risks; however, as of October 2018, the Secretaries had used this authority only once.²⁰

²⁰ (U) Public Law 111-383, “NDAA for FY 2011,” January 7, 2011. (Section 806 is now Section 2339a, title 10, United States Code, 2018.)

(U) In March 2018, the DoD enhanced its procedures to proactively address supply chain threats and block the procurement of risky products for national security systems, referred to as the “NSS-restricted list” and used DoD’s Section 2339a authority to prohibit the purchase of one back-up and disaster recovery product. However, this list and the authority granted by Congress only applies to national security systems, allowing these products to be used on all other DoD systems. Implementing and using the NSS-restricted list across the DoD, not just for NSSs, would help prevent the purchase of COTS information technology items with cybersecurity risks across the DoD. The USD(A&S) and DoD CIO should identify and implement administrative solutions, such as expanding the DoD’s implementation of its current 10 U.S.C. 2339a authorities, and if those solutions are insufficient to address the issues identified in this report, seek legislative authority to expand the NSS-restricted list DoD-wide to include high-risk COTS information technology items used for non-national security systems.

(U) Using COTS Items With Cybersecurity Risks Weakens National Security

~~(U//FOUO)~~ As a result, the DoD increased the risk that adversaries could exploit known cybersecurity vulnerabilities. If the DoD continues to purchase and use COTS information technology items without identifying, assessing, and mitigating known vulnerabilities associated with COTS information technology items, missions critical to national security could be compromised. For example, the Department of State issued a warning in May 2017 against using Hangzhou Hikvision Digital Technology Company and Dahua Technology Company video surveillance equipment, citing cyberespionage concerns from China. Despite the inherent risks associated with their use, DoD Components continued to purchase and use these COTS items to monitor installation security until Congress banned the Federal Government from using them in August 2018. In addition, despite reports from the [REDACTED]

[REDACTED], DoD Components purchased and used the systems to [REDACTED]. Using COTS information technology items, [REDACTED]

(U) The DoD's reliance on a wide variety of COTS information technology items and the integration of those items into nearly all DoD systems and networks necessitates a DoD-wide effort to ensure that cybersecurity risks associated with COTS information technology items are identified, assessed, and mitigated before they compromise missions critical to national security. Purchasing secure COTS information technology items, while initially more costly, would decrease the risk of adversaries exploiting vulnerabilities that could compromise operations and should lower the overall cost of ownership by reducing the necessity to replace unsecure COTS information technology items that are later banned for use or pose unacceptable cybersecurity risks to the DoD.²¹ For example, the DoD and other Federal agencies have had to identify and replace all hardware and software that contain Kaspersky Lab software on their networks with technology that has not been banned for use by the Federal Government. This process has resulted in the DoD expending resources to replace all products with Kaspersky Lab software.

(U) Purchasing secure COTS information technology items should lower the overall cost of ownership by reducing the necessity to later replace unsecure COTS information technology items.

(U) In addition, the interconnectivity of COTS information technology devices provides adversaries the opportunity to compromise missions or operations by exploiting the cybersecurity vulnerabilities of only one of many connected devices. In July 2017, the Government Accountability Office reported that the DoD had not yet conducted the required assessments of how its use of Internet-connected COTS information technology devices affected its operations, and that DoD cybersecurity, information security, physical security, and operations security policies did not sufficiently address the use of these devices.²² The DoD continues to increase its risk that adversaries could exploit known cybersecurity risks each time it purchases and uses a COTS information technology item without identifying, assessing, and mitigating known vulnerabilities associated with high-risk COTS information technology items.

²¹ (U) The MITRE Corporation Report, "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," August 2018.

²² (U) Government Accountability Office Report No. GAO-17-668, "IoT: Enhanced Assessments and Guidance are Needed to Address Security Risks in DoD," July 2017.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the Secretary of Defense direct an organization or group to develop a:

- a. (U) Risk-based approach to prioritize commercial off-the-shelf items for further evaluation.
- b. (U) Process to test high-risk commercial off-the-shelf items.
- c. (U) Process to prohibit the purchase and use of high-risk commercial off-the-shelf items, when necessary, until mitigation strategies can limit the risk to an acceptable level.

(U) Acting Secretary of Defense Comments

(U//FOUO) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. Those comments are addressed below.

(U) USD(A&S) and DoD CIO Comments

(U//FOUO) Although not required to comment, the USD(A&S) and DoD CIO stated that the DoD would [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

(U//FOUO) The Under Secretary and DoD CIO also stated that [REDACTED]
[REDACTED]. Based on those requirements, the Under Secretary and DoD CIO stated that they, in coordination with U.S. Cyber Command, Under Secretary of Defense for Research and Engineering, and the Military Departments, [REDACTED]
[REDACTED]. The Under Secretary and DoD CIO also stated that the [REDACTED]

(U//FOUO) [REDACTED]
[REDACTED]
[REDACTED]. In addition, the Under Secretary and DoD CIO stated that, when warranted [REDACTED]
[REDACTED].

(U//FOUO) The Under Secretary and DoD CIO acknowledged that [REDACTED]
[REDACTED]
[REDACTED]. The Under Secretary and DoD CIO pointed out that [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].²³ They stated that Congress has already recognized the need for greater authority [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].²⁴ The Under Secretary and DoD CIO also stated that [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. Therefore, the Under Secretary and DoD CIO stated that they [REDACTED]
[REDACTED]
[REDACTED] as described in their response to Recommendation 4.

(U) Our Response

(U) Comments from the Acting Secretary of Defense, USD(A&S), and DoD CIO did not address the specifics of the recommendations; therefore, the recommendations are unresolved. We acknowledge that DoD policies and procedures address supply chain risk management in acquisition decisions and require the DoD to identify, assess, and mitigate cybersecurity risks. However, as stated in the report, responsibility for identifying, testing, and mitigating cybersecurity risks is decentralized among many organizations with overlapping responsibilities. As shown in the report, the current risk-based approach is not effective at identifying DoD-wide high-risk COTS items; therefore, we consider Recommendation 1.a unresolved.

²³ (U) Section 253, title 41, United States Code, 1984.

²⁴ (U) Public Law 115-390, "The Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act," December 21, 2018.

(U) We also acknowledge that the DoD has testing and analysis organizations, such as the Joint Federated Assurance Center; however, as stated in the report, Joint Federated Assurance Center support is limited because the Center is not fully operational. In addition, there is no requirement to use the Center for testing or to follow the Center's recommendations, and the Center is not required to share test results across the DoD. Despite DoD policies and the numerous organizations performing cybersecurity testing and analysis, there appears to be no organization assessing the risks for COTS items DoD-wide, identifying high-risk items for further testing, or actively recommending prohibition of these high-risk items when necessary. Therefore, we consider Recommendation 1.b unresolved.

(U//FOUO) [REDACTED]
[REDACTED]
[REDACTED]. We also agree that the [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. However, the DoD has not introduced guidance to [REDACTED]
[REDACTED]. Therefore, we consider Recommendation 1.c unresolved.

(U) The Acting Secretary of Defense, USD(A&S), or DoD CIO, should provide additional comments on the final report that address actions to resolve the recommendations.

(U) Recommendation 2

(U) We recommend that the Under Secretary of Defense for Acquisition and Sustainment update:

- a. **(U) Existing DoD acquisition policies or develop and implement new policy to require organizations to review and evaluate cybersecurity risks, including supply chain and counterintelligence risks, for high-risk commercial off-the-shelf items prior to purchase, regardless of purchase method.**

(U) USD(A&S) Comments

(U//FOUO) The USD(A&S) agreed, stating that [REDACTED]

[REDACTED].²⁵ The Under Secretary noted that DoD policies, including DoD Instructions 5000.01, 5000.02, 5200.44, 8510.01, and 5200.39, require [REDACTED]

[REDACTED]²⁶ The Under Secretary stated that [REDACTED]

(U) Our Response

(U) Comments from the USD(A&S) addressed all specifics of the recommendation; therefore, the recommendation is resolved but remains open. We will close the recommendation once the USD(A&S) provides the updated version of DoD Instruction 5200.44 and we verify that it addresses requirements for evaluating COTS items cybersecurity risks prior to their purchase, regardless of the purchase method.

- b. (U) Government purchase card program policy and training to include training on common cybersecurity risks, including supply chain and counterintelligence risks, for commercial off-the-shelf information technology items and the impact of the risks to the mission.**

(U) USD(A&S) Comments

(U//FOUO) The USD(A&S) agreed, stating that the USD(A&S) would [REDACTED]

[REDACTED]. The Under Secretary stated that [REDACTED]

²⁵ (U) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012 (Incorporating Change 3, October 15, 2018).

²⁶ (U) DoD Instruction 5000.01, "The Defense Acquisition System," May 12, 2003 (Incorporating Change 2, August 31, 2018); DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015 (Incorporating Change 2, October 15, 2018).

(U) Our Response

(U) Comments from the USD(A&S) addressed all specifics of the recommendation; therefore, the recommendation is resolved but remains open. We will close the recommendation once the USD(A&S) provides updated GPC policy and training requirements and we verify the policy and training requirements address the COTS information technology supply chain and counterintelligence risks.

(U) Recommendation 3

(U) We recommend that the DoD Chief Information Officer revise DoD Instruction 8100.04, “DoD Unified Capabilities (UC),” December 9, 2010, to require an assessment of supply chain risks as a condition for approval to be included on the Unified Capabilities approved products list.

(U) DoD CIO Comments

~~(U//FOUO)~~ The DoD CIO agreed, stating that his office would [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED].

(U) Our Response

(U) Comments from the DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but remains open. We will close the recommendation once the DoD CIO provides the updated issuance of DoD Instruction 8100.04 and verify that it requires an assessment of supply chain risk management as part of the approval process for including products on the APL.

(U) Recommendation 4

(U) We recommend that the Under Secretary of Defense for Acquisition and Sustainment and the DoD Chief Information Officer identify and implement administrative solutions, such as expanding the DoD’s implementation of its current section 2339a, title 10, United States Code, 2018, authorities and, if those solutions are insufficient to address the issues identified in this report, seek legislative authority to expand the national security system-restricted list DoD-wide to include high-risk commercial off-the-shelf information technology items used for non-national security systems.

(U) USD(A&S) and DoD CIO Comments

(U//FOUO) The USD(A&S) and DoD CIO agreed, stating that, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].²⁷ The Under Secretary and DoD CIO also stated
that the [REDACTED]
[REDACTED]
[REDACTED]. Furthermore, the Under Secretary and DoD CIO
stated that the DoD CIO would issue [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

(U) Our Response

(U) Comments from the USD(A&S) and DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved and closed. We agree that the SECURE Technology Act and Executive Order 13873 provides the DoD the authority that they need to expand the national security system-restricted list DoD-wide. The enhanced procedures to improve DoD's implementation will be reviewed with the response to Recommendation 1.c, which recommends that the Secretary of Defense direct an organization to develop a process to prohibit the purchase and use of high-risk COTS items.

²⁷ (U) Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from March 2018 through May 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) Scope of UAS Work

(U) Our original audit objective was to determine whether the DoD implemented and operated cyber and physical security controls in accordance with Federal and DoD system, communications, and information security requirements to protect select unmanned aerial vehicle systems from unauthorized access and use.²⁸ We met with officials from the USD(A&S) and the DoD CIO responsible for acquisition and cybersecurity for UASs. In addition, we met with officials from the Naval Air Systems Command and Air Force Life Cycle Management Center responsible for overseeing the Services' UAS program offices and provides management of weapons systems throughout their life cycles.

(U) We visited the Army Program Executive Office, Aviation at Redstone Arsenal in Huntsville, Alabama; the Naval Air Warfare Center Aircraft Division at Naval Air Station Patuxent River in Patuxent River, Maryland; and the Air Force Life Cycle Management Center, Medium Altitude UAS Division, at Wright-Patterson Air Force Base in Dayton, Ohio. During these site visits, we met with officials responsible for managing and securing individual UAS programs and data communications; managing UAS contracts for, among other areas, maintenance and repairs; managing UAS inventories; and ensuring that UASs met air worthiness requirements.²⁹ At these sites, we also met with officials responsible for assessing UAS threats and cybersecurity risks. In addition, we visited the U.S. Air Force Special Operations Command at Hurlburt Field in Mary Esther, Florida, and met with officials responsible for capability development and integration of small UASs for the Air Force.

²⁸ (U) A UAS includes all necessary equipment, networks, and personnel to control an unmanned aerial vehicle.

²⁹ (U) Airworthiness is the measure of an aircraft's suitability for safe flight.

(U) We also met with officials from the Director, Operational Test and Evaluation responsible for providing operational testing and analysis of weapon systems, including larger UAS programs. In addition, we met with officials from the National Security Agency, Defense Innovation Unit, and the National Ground Intelligence Center responsible for researching and evaluating UAS cybersecurity risks and vulnerability mitigation solutions.

(U//FOUO) We obtained and reviewed UAS briefings and threat assessments; plans of action and milestones to address UAS vulnerabilities; incident reports; and vulnerability reports issued by [REDACTED]

[REDACTED]. In addition, we also obtained and reviewed Federal, DoD, and Army, Navy, and Air Force cybersecurity and acquisition policies; the [REDACTED]; and the DoD Government Charge Card Guidebook for Establishing and Managing Purchase, Travel, and Fuel Card Programs.

(U//FOUO) Based on initial audit work, we identified [REDACTED], which resulted in our issuance of a notice of concern. While the DoD took action to address our concerns, we reannounced the audit with a broader objective focused on the cybersecurity risks associated with COTS items.

(U) Scope of COTS Items Work

(U) We met with USD(A&S) and DoD CIO officials responsible for developing acquisition policy and GPC training requirements, establishing supply chain risk management policy and procedures, and restricting GPC purchases. In addition, we met with Defense Information Systems Agency Assessments and Authorizations Division officials to discuss the process for approving products for inclusion on an APL. Furthermore, we met with officials from the Defense Intelligence Agency Supply Chain Risk Management Threat Assessment Center responsible for collecting intelligence and developing supply chain threat assessments.

(U) We also met with officials from the Offices of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology and Air Force Chief Information Officer; and the Naval Surface Warfare Center, Dahlgren, responsible for acquisition, testing, analysis, and sharing the cybersecurity risks of COTS items. We met with officials from the Office of the Under Secretary of Defense for Research and Engineering, Joint Federated Assurance Center responsible for coordinating hardware and software assurance policies, testing, and standards across the DoD. In addition, we met with officials from

(U) the U.S. Army Program Executive Office, Enterprise Information Systems, responsible for managing the Army's Computer Hardware, Enterprise Software and Solutions system and the Air Force Life Cycle Management Center, Program Executive Office responsible for managing contracts used by GPC holders to purchase COTS information technology items.

(U) We obtained and reviewed congressional testimony; the DoD Unified Capabilities APL; Department of Homeland Security advisories; and DoD, Army, Navy, and Air Force GPC policy, procedures, and training requirements. We also reviewed the Federal Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, and international commercial items standards. In addition, we reviewed the National Institute of Standards and Technology's National Vulnerabilities Database to identify COTS items with known cybersecurity risks and vendors associated with providing the COTS items. Furthermore, we obtained and reviewed GPC purchase extracts from the Army's Computer Hardware Enterprise Software and Solutions System and the Air Force's portal to identify GPC COTS items purchases during FY 2018. We focused our review of COTS items from vendors such as Lenovo, Lexmark, and GoPro and items such as televisions, security cameras, and printers that had known cybersecurity risks.

(U) Use of Computer-Processed Data

(U) We used computer-processed data from the Army's Computer Hardware, Enterprise Software and Solutions to identify COTS information technology items purchased by Army GPC holders. The Army uses the Computer Hardware, Enterprise Software, and Solutions systems to manage COTS information technology purchases of hardware and software made using multiple award, indefinite-delivery indefinite-quantity contracts. We also used computer-processed data from Air Force vendors supporting the Air Force's Network-Centric Solutions-2 Products and Information Technology Commodity Council contracts that the Air Force Life Cycle Management Center provided to identify COTS information technology items purchased by Air Force personnel. Although the Air Force uses the Air Force Way portal to manage its information technology contracts, the portal shows both requests for pricing and COTS information technology purchases. Reports generated using the Air Force Way portal do not separate the different types of transactions.

(U) To assess the reliability of the data, we interviewed the Computer Hardware, Enterprise Software, and Solutions product lead, Network-Centric Solutions-2 Products deputy program manager, and the Deputy Director of the Information Technology Commodity Council to discuss known weaknesses in the systems. We identified internal control deficiencies that allowed users to purchase COTS information technology items without using the established contracts in the systems; therefore, the data was incomplete. Although we identified discrepancies with the data, we

(U) determined that the Army's data was sufficiently reliable to identify whether its GPC holders purchased COTS information technology items with known cybersecurity weaknesses. For the Air Force, we also identified problems with the accuracy of the information because it combined requests for pricing with actual purchases made. Therefore, we could not rely on the Air Force data to identify the number and value of COTS information technology items purchases for its GPC holders.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) issued one report on COTS items cybersecurity risks related to IoT device use.

(U) GAO

(U) GAO-17-668, "IoT: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DoD," July 2017

(U) The GAO reported that, although the DoD had begun to examine security risks of IoT devices through infrastructure-related and intelligence assessments, the DoD had not conducted required assessments on how its use of IoT devices affected operations. Specifically, the GAO identified that DoD cybersecurity, information security, physical security, and operations security policy did not sufficiently address the use of IoT devices.

(U) Appendix B

(U//FOUO)



~~SECRET//NOFORN//LES~~
INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

MAY 3 4 2018

ACTION MEMO

FOR: SECRETARY OF DEFENSE

FROM: Glenn A. Fine, Principal Deputy Inspector General, Performing the Duties of the
Inspector General

(U) RECOMMENDATION: We request that you respond to these suggested actions or provide alternative actions taken within 10 calendar days of the issuance of this notice of concern.

COORDINATION: None

Attachment(s):
As stated.

Cc:
Deputy Secretary of Defense
Secretary of the Army
Secretary of the Navy
Secretary of the Air Force
Under Secretary of Defense for Research and Engineering
Department of Defense Chief Information Officer

~~SECRET//NOFORN//LES~~

~~This document is FOUO when separated from attachment~~

~~(U//FOUO)~~



~~SECRET//NOFORN//LES~~

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

MAY 14 2018

(U) MEMORANDUM FOR SECRETARY OF DEFENSE
DEPUTY SECRETARY OF DEFENSE
SECRETARY OF THE ARMY
SECRETARY OF THE NAVY
SECRETARY OF THE AIR FORCE
UNDER SECRETARY OF DEFENSE FOR RESEARCH AND
ENGINEERING
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF
DEFENSE

Classified by: [REDACTED]
Derived from: Multiple Sources
Declassify on: 50X1-HUM

~~SECRET//NOFORN//LES~~

(U//FOUO)

~~SECRET//NOFORN//LEG~~

2

~~SECRET//NOFORN//LEG~~

(U//FOUO)

~~SECRET//NOFORN//LES~~

3

~~SECRET//NOFORN//LES~~

~~(U//FOUO)~~



~~SECRET//NOFORN//LES~~

4



~~SECRET//NOFORN//LES~~

(U//FOUO)

~~SECRET//NOFORN//LES~~

5

(U) Suggested Actions

(U) Please respond to these suggested actions or provide alternative actions taken within 10 calendar days of the issuance of this notice of concern. The points of contact for your responses are

This memorandum and management comments on the suggested actions will be included in the final audit report.




Glenn A. Fine
Principal Deputy Inspector General
Performing the Duties of the Inspector General

~~SECRET//NOFORN//LES~~

(U) Appendix C

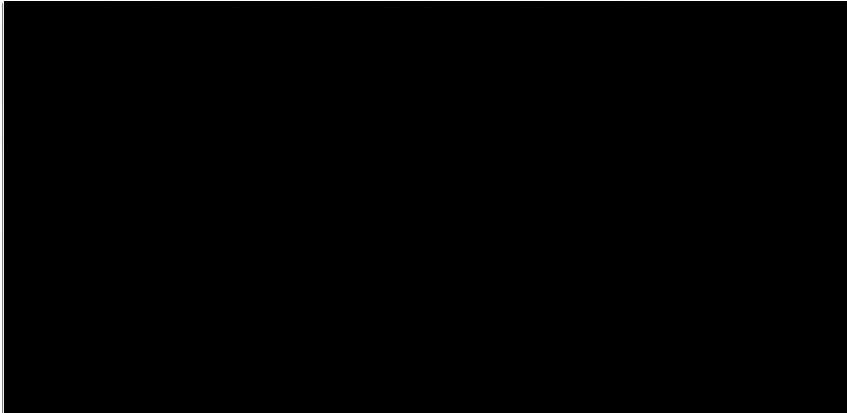
(U//FOUO)


~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~


 **DEPUTY SECRETARY OF DEFENSE**
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010


MAY 23 2018

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF
DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM
EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF
DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE
AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC
AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES








OSD070728-18/CMD071139-18

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U//FOUO)



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

JUN - 1 2018

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF
DEFENSE

SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF, NATIONAL GUARD BUREAU
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM
EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF
DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE
AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC
AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

Attachment:
As stated



OSD007197-18/CMD009069-18

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U//FOUO)



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JUN - 1 2018

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF
DEFENSE

SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF, NATIONAL GUARD BUREAU
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM
EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF
DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE
AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC
AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

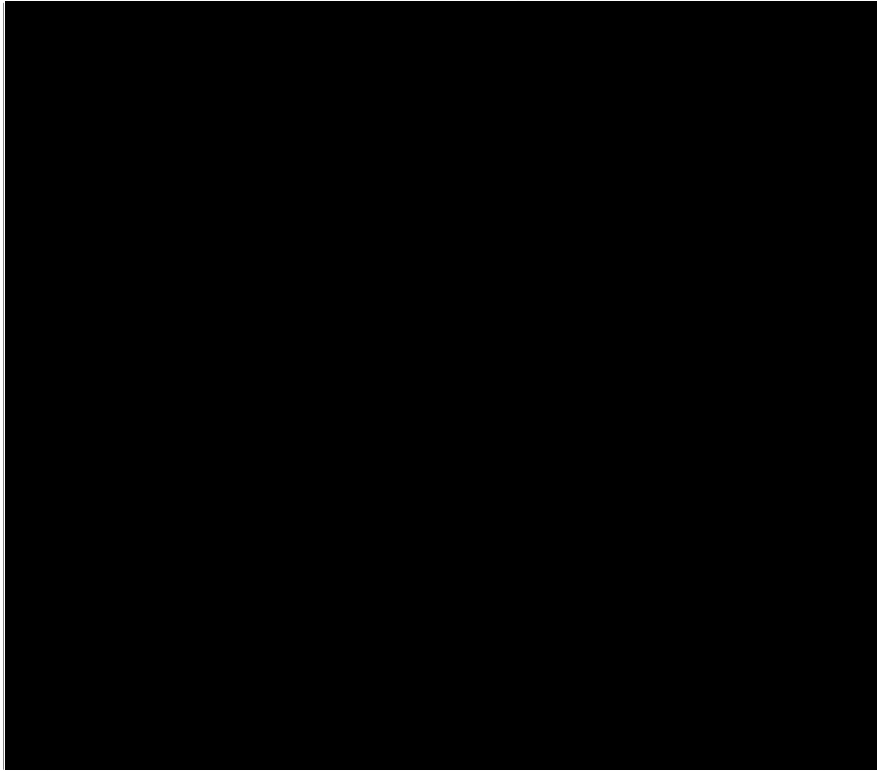
(U//FOUO)


~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~


~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U//FOUO)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~




Dana Deasy
Department of Defense
Chief Information Officer


Ellen M. Lord
Under Secretary of Defense for
Acquisition and Sustainment

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U) Appendix D

(U) Banned or Restricted COTS Items and Manufacturers

U//FOUO Item/Manufacturer	Risk/Threat	Ban/Warning/Restriction
Video surveillance equipment from Hangzhou Hikvision Digital Technology Company and Dahua Technology Company	Cyberespionage risk; unauthorized system or network access; and Chinese government ownership, control, or influence	In May 2017, the Department of Homeland Security issued an advisory that included concerns with using these items. In August 2018, Congress banned the purchase and use of these COTS items. ¹
Telecommunications equipment from Hytera Communications Corporation	Cyberespionage risk	In August 2018, Congress banned the purchase of these COTS items. ²
Geolocation-capable devices, applications, and services	Exposure of sensitive locations, routines, and personal information	In August 2018, the Deputy Secretary of Defense banned these COTS items from being used in operational areas. ³
Personal and Government mobile devices	Cyberespionage risk and unauthorized disclosure of classified information	In May 2018, the Deputy Secretary of Defense banned these COTS items from secure spaces. ⁴
[REDACTED]	[REDACTED]	[REDACTED] ⁵
Telecommunications equipment from Huawei Technologies Company and ZTE Corporation	Cyberespionage risk and Chinese government ownership, control, or influence	In October 2012, the U.S. House of Representatives Permanent Select Committee on Intelligence issued a report that identified vulnerabilities with use of these COTS items. ⁶ In December 2017, Congress banned the purchase and use of these COTS items. ⁷ In April 2018, the DoD banned the sale of these COTS items at military exchanges.
Hardware, software, and services from Kaspersky Lab	Cyberespionage risk; unauthorized system or network access; and Russian government ownership, control, or influence	In September 2017, the Department of Homeland Security banned the purchase and use of these COTS items, and U.S. Cyber Command removed these COTS items from DoD networks. ⁸ In December 2017, Congress banned the purchase and use of these COTS items. ⁹

U//FOUO

U//FOUO Item/Manufacturer	Risk/Threat	Ban/Warning/Restriction
Computers from Lenovo	Cyberespionage risk; unauthorized system or network access; and Chinese government ownership, control, or influence	In May 2006, the Department of State banned the purchase and use of these COTS items on State Department classified networks.
		In February and August 2015, the Department of Homeland Security issued cybersecurity vulnerability alerts for these COTS items.
		In September 2016, a DoD Joint Chiefs Intelligence Directorate report identified cyberespionage risks for these COTS items.
Removable media devices	Unauthorized disclosure of classified information and spread of malware	In November 2008, U.S. Strategic Command banned the use of these COTS items on DoD networks.
		In February 2010, U.S. Strategic Command removed the ban of these COTS items.
		In December 2010, U.S. Strategic Command reinstituted the ban for using these COTS items on classified networks.

U//FOUO


- ¹ (U) Public Law 115-232, "NDAA for Fiscal Year 2019," Title VII, "Acquisition Policy, Acquisition Management, and Related Matters," Subtitle H, "Other Matters," Section 889, August 13, 2018.
- ² (U) Public Law 115-232, "NDAA for Fiscal Year 2019," Title VII, "Acquisition Policy, Acquisition Management, and Related Matters," Subtitle H, "Other Matters," Section 889, August 13, 2018.
- ³ (U) Deputy Secretary of Defense Memorandum, "Use of Geolocation-Capable Devices, Applications, and Services," August 3, 2018.
- ⁴ (U) Deputy Secretary of Defense Memorandum, "Mobile Device Restrictions in the Pentagon," May 22, 2018.
- ⁵ (U//FOUO) [REDACTED]
- ⁶ (U) Permanent Select Committee on Intelligence, U.S. House of Representatives, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," October 8, 2012.
- ⁷ (U) Public Law 115-91, "NDAA for Fiscal Year 2018," Title XVI, "Strategic Program, Cyber, and Intelligence Matters," Subtitle D, "Cyberspace-Related Matters," Section 1656, December 12, 2017.
- ⁸ (U) Department of Homeland Security Binding Operational Directive 17-01, "Removal of Kaspersky-Branded Products," September 13, 2017.
- ⁹ (U) Public Law 115-91, "NDAA for Fiscal Year 2018," Title XVI, "Strategic Program, Cyber, and Intelligence Matters," Subtitle C, "Cyberspace-Related Matters," Section 1634, December 12, 2017.

(U) Source: The DoD OIG.

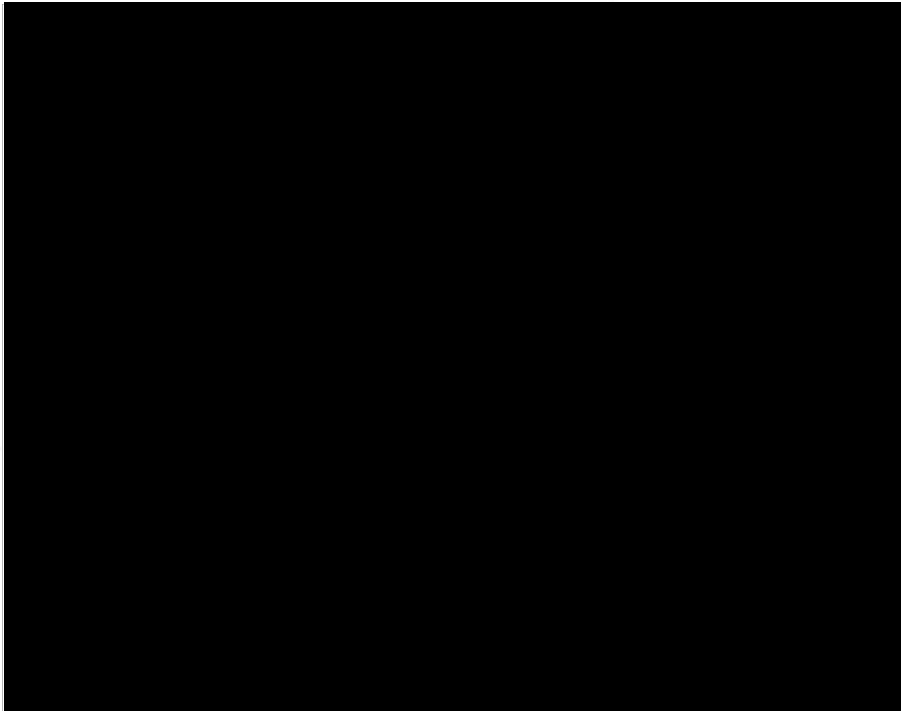
(U) Management Comments

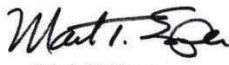
(U) Acting Secretary of Defense

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

 **SECRETARY OF DEFENSE**
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

7/8/19

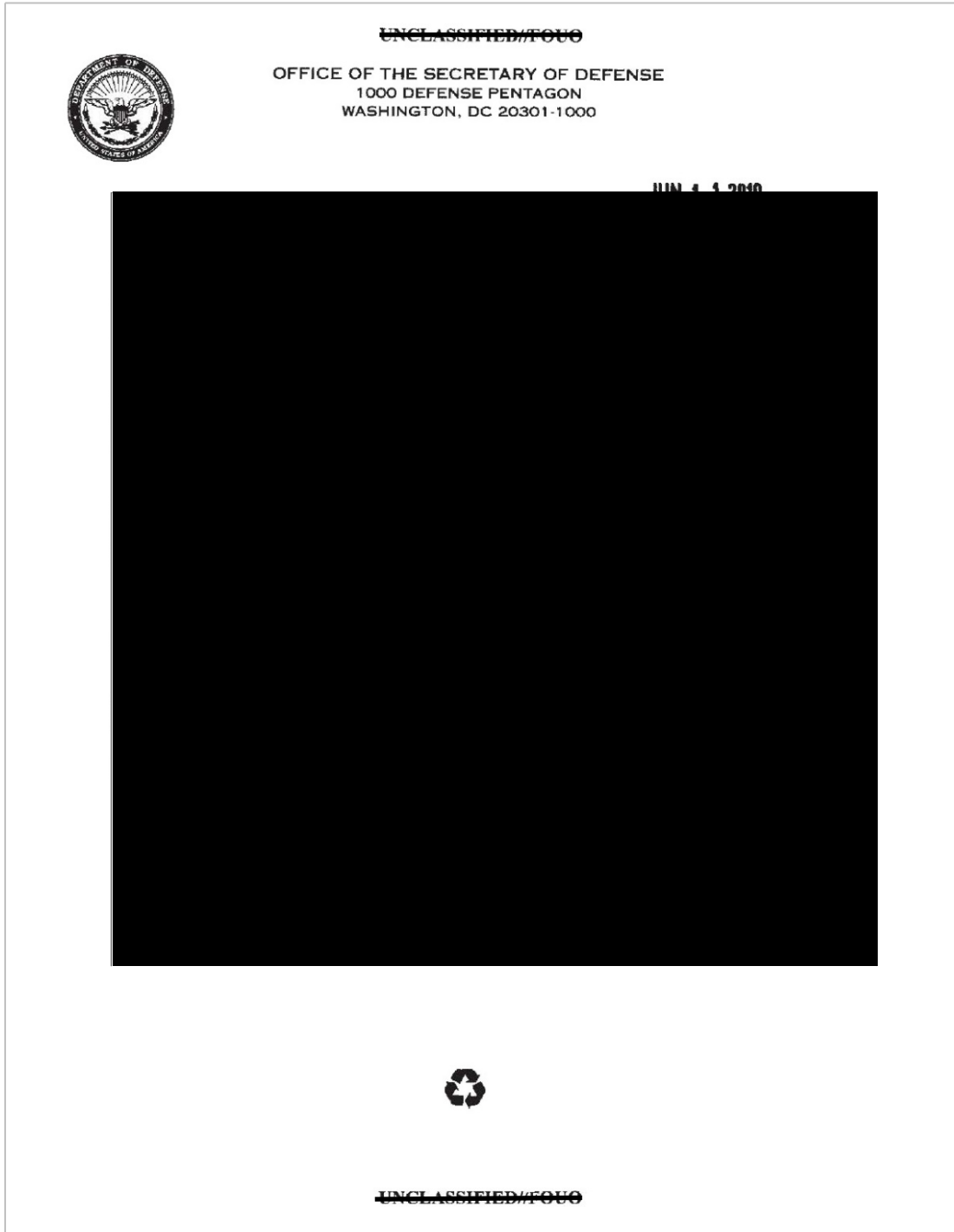



Mark T. Esper
Acting

Enclosure:
As stated

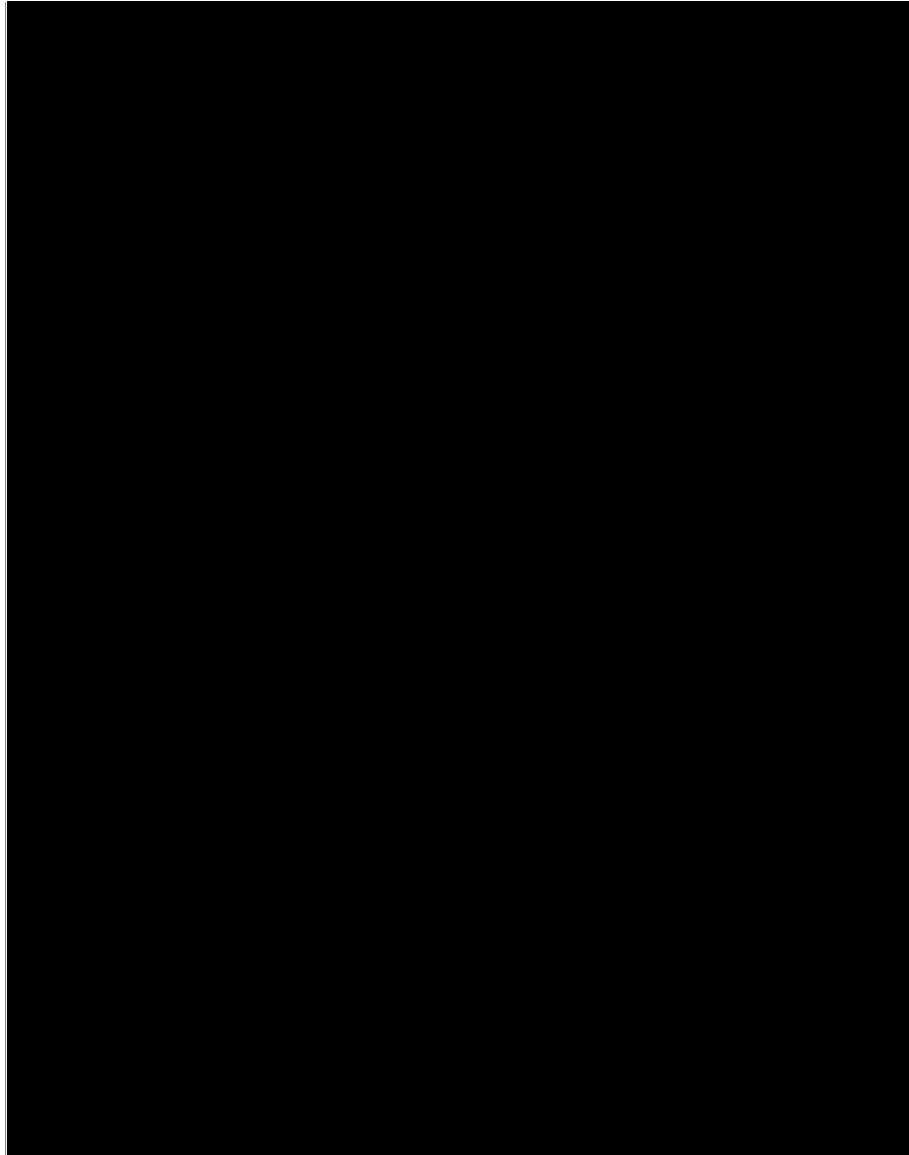
~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U) Undersecretary of Defense for Acquisitions and Sustainment and DoD Chief Information Officer



(U) Undersecretary of Defense for Acquisitions and Sustainment and DoD Chief Information Officer (cont'd)

~~UNCLASSIFIED//FOUO~~



2

~~UNCLASSIFIED//FOUO~~

(U) Undersecretary of Defense for Acquisitions and Sustainment and DoD Chief Information Officer (cont'd)

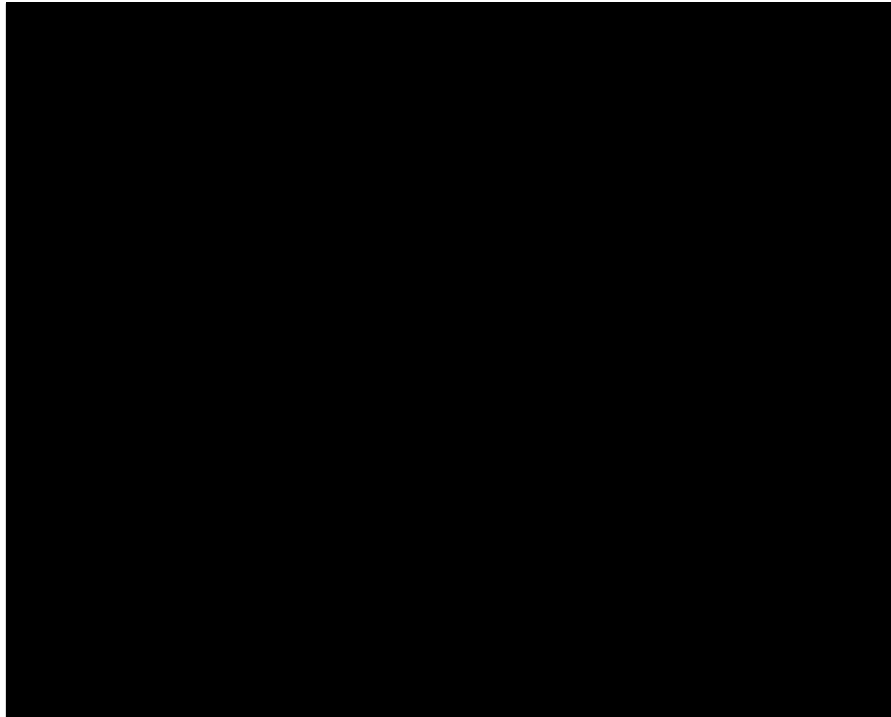
~~UNCLASSIFIED//FOUO~~



~~UNCLASSIFIED//FOUO~~

(U) Undersecretary of Defense for Acquisitions and Sustainment and DoD Chief Information Officer (cont'd)

~~UNCLASSIFIED//FOUO~~



(U) The Department appreciates the effort of the DoD IG and the opportunity to comment on the final report. The point of contact for Office of Secretary of Defense Acquisition and Sustainment is [REDACTED] and the point of contact for the Department of Defense Chief Information Office is [REDACTED]

Ellen M. Lord

ELLEN M. LORD
Under Secretary of Defense
for Acquisition and Sustainment

Danas Deasy

DANAS. DEASY
Department of Defense
Chief Information Officer

Enclosure:
As stated

~~UNCLASSIFIED//FOUO~~

(U) Acronyms and Abbreviations

APL	Approved Products List
CIO	Chief Information Officer
COTS	Commercial off-the-shelf
DJI	Da Jiang Innovation
GPC	Government Purchase Card
IoT	Internet of Things
NDAA	National Defense Authorization Act
NSS	National Security System
UAS	Unmanned Aircraft System
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment

(U) Glossary

(U) **Commercial Item.** Articles of supply readily available from established commercial distribution sources which the Department of Defense or inventory managers in the Military Services have designated to be obtained directly or indirectly from such sources.

(U) **Commercial Off-The-Shelf (COTS).** A commercial item sold in substantial quantity in the commercial marketplace that is offered to the government in the same form in which it is sold in the marketplace

(U) **Cyberespionage.** The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization.

(U) **Internet of Things (IoT).** The Internet of Things is the set of Internet Protocol-addressable devices that interact with the physical environment. IoT devices typically contain elements for sensing, communications, computational processing, and actuation.

(U) **National Security System (NSS).** Any information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency the function, operation, or use of which:

- (U) involves intelligence activities;
- (U) involves cryptologic activities related to national security;
- (U) involves command and control of military forces;
- (U) involves equipment that is an integral part of a weapon or weapon system; or
- (U) is critical to the direct fulfillment of military or intelligence missions; or
- (U) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(U) **Program of Record.** A program as recorded in the current Future Years Defense Program or as updated from the last Future Years Defense Program by approved program documentation. May also refer to a program having successfully achieved the development decision that commits the resources needed to conduct development leading to production and fielding of the product.

(U) **Supply Chain Risk.** The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

(U) **Supply Chain Risk Management.** A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

(U) **Unmanned Aerial Vehicle.** A powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload.

(U) **Unmanned Aircraft System (UAS).** That system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft.

(U) Annex: Classified Source

[REDACTED]
[REDACTED]
[REDACTED] (Classified SECRET//NOFORN)

(U) Declassification Date: 50X1-HUM

(U) Generated Date: May 14, 2018

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible waste, fraud, and abuse in government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

~~SECRET//NOFORN~~



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098

~~SECRET//NOFORN~~