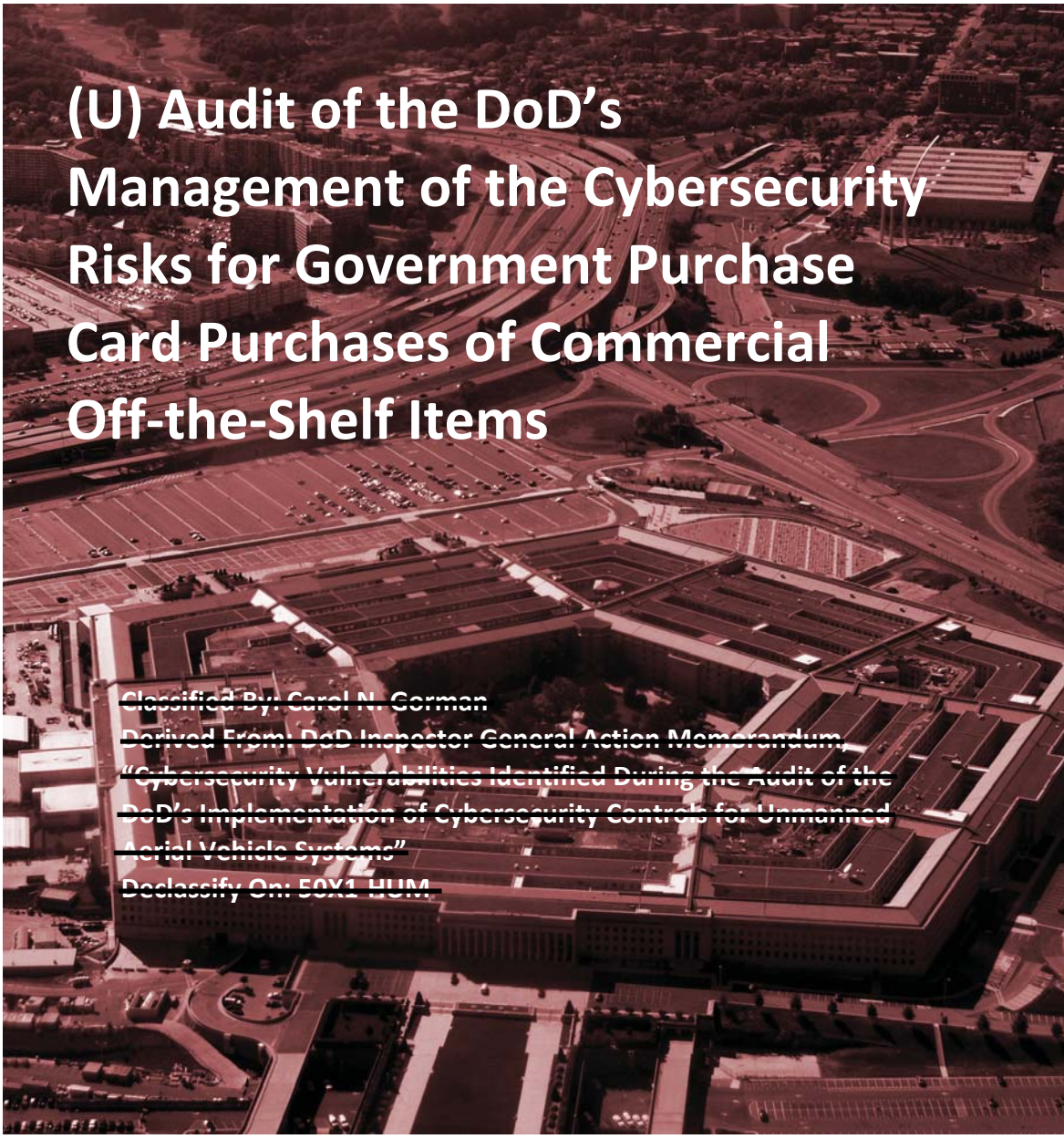
Report No. DODIG-2019-106

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

# (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

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

~~(U//FOUO)~~ [redacted]

# (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].[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]. 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].

(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.

## *(U) Recommendations Table*

| Unclassified<br>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<br>**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*

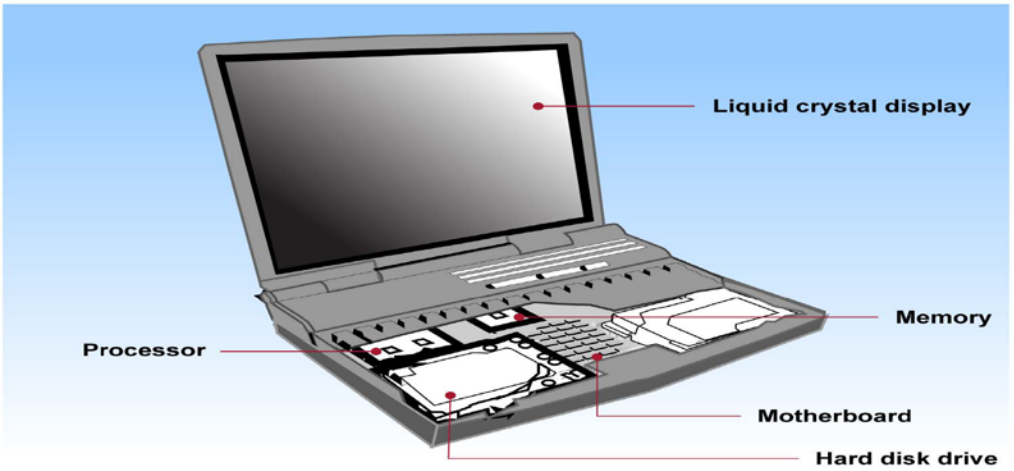
(U) Federal agencies have reported cybersecurity risks associated with using COTS information technology items, such as:

- (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*




| Component | Location of facilities potentially used by suppliers |
|---|---|
| **Liquid crystal display** | China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan |
| **Memory** | China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States |
| **Processor** | Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam |
| **Motherboard** | Taiwan |
| **Hard disk drive** | China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States |

Source: GAO analysis of public information. | GAO-18-667T

## (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], 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)~~ [redacted]

~~(S//NF)~~ [redacted]. On May 14, 2018, we issued a notice of concern to the Secretary of Defense, [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]. For example, [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], the DoD did not take steps to [redacted]. This occurred because [redacted]. We suggested that the Secretary of Defense issue a [redacted].

~~(S//NF)~~ On May 23, 2018, the Deputy Secretary of Defense [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].

## (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] 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] 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.

**(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.**

[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]. According to the DoD CIO Deputy Director for Cybersecurity Risk Management, [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//FOUO)~~ [redacted].

## *(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 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]

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

[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], 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]. 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].

~~(U//FOUO)~~ The Under Secretary and DoD CIO also stated that [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]. The Under Secretary and DoD CIO also stated that the [redacted]

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

~~(U//FOUO)~~ The Under Secretary and DoD CIO acknowledged that [redacted]. The Under Secretary and DoD CIO pointed out that [redacted].[23] They stated that Congress has already recognized the need for greater authority [redacted].[24] The Under Secretary and DoD CIO also stated that [redacted]. Therefore, the Under Secretary and DoD CIO stated that they [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]. We also agree that the [redacted]. However, the DoD has not introduced guidance to [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].[25] The Under Secretary noted that DoD policies, including DoD Instructions 5000.01, 5000.02, 5200.44, 8510.01, and 5200.39, require [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]. 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].

### *(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].[27] The Under Secretary and DoD CIO also stated that the [redacted]. Furthermore, the Under Secretary and DoD CIO stated that the DoD CIO would issue [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]. 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)~~ [redacted]

~~SECRET//NOFORN//LES~~

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

MAY 14 2018

ACTION MEMO

FOR: SECRETARY OF DEFENSE

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

[redacted]

(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

[redacted]

~~SECRET//NOFORN//LES~~
~~This document is FOUO when separated from attachment~~

~~(U//FOUO)~~ [redacted]

~~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

[redacted]

[redacted]

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

~~SECRET//NOFORN//LES~~

~~(U//FOUO)~~ [redacted]

~~SECRET//NOFORN//LES~~

2

[redacted]

~~SECRET//NOFORN//LES~~

~~(U//FOUO)~~ [redacted]

~~SECRET//NOFORN//LES~~

3

[redacted]

~~SECRET//NOFORN//LES~~

~~(U//FOUO)~~ [redacted]

~~SECRET//NOFORN//LES~~

4

[redacted]

~~SECRET//NOFORN//LES~~

~~(U//FOUO)~~ [redacted]

~~SECRET//NOFORN//LES~~

5

[redacted]

**(U) Suggested Actions**

[redacted]

(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 [redacted]. 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)~~ [redacted]

~~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

[redacted]

OSD070728-18/CMD071139-18

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~(U//FOUO)~~ [redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

[redacted]

Attachment:
As stated

OSD007197-18/CMD009069-18

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~(U//FOUO)~~ [redacted]

~~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

[redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~(U//FOUO)~~ [redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

[redacted]

2

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~(U//FOUO)~~ [redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

[redacted]

Dana Deasy
Department of Defense
Chief Information Officer

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

3

~~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<br><br>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]<br>~~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

[redacted]

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

~~UNCLASSIFIED//FOUO~~

OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JUN 4 1 2019

[redacted]

~~UNCLASSIFIED//FOUO~~

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

~~UNCLASSIFIED//FOUO~~

[redacted]

2

~~UNCLASSIFIED//FOUO~~

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

~~UNCLASSIFIED//FOUO~~

[redacted]

3

~~UNCLASSIFIED//FOUO~~

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

~~UNCLASSIFIED//FOUO~~

[redacted]

(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 Sectary 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
Under Secretary of Defense
for Acquisition and Sustainment

for DANA S. DEASY
Department of Defense
Chief Information Officer

Enclosure:
As stated

4

~~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] (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/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil*

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

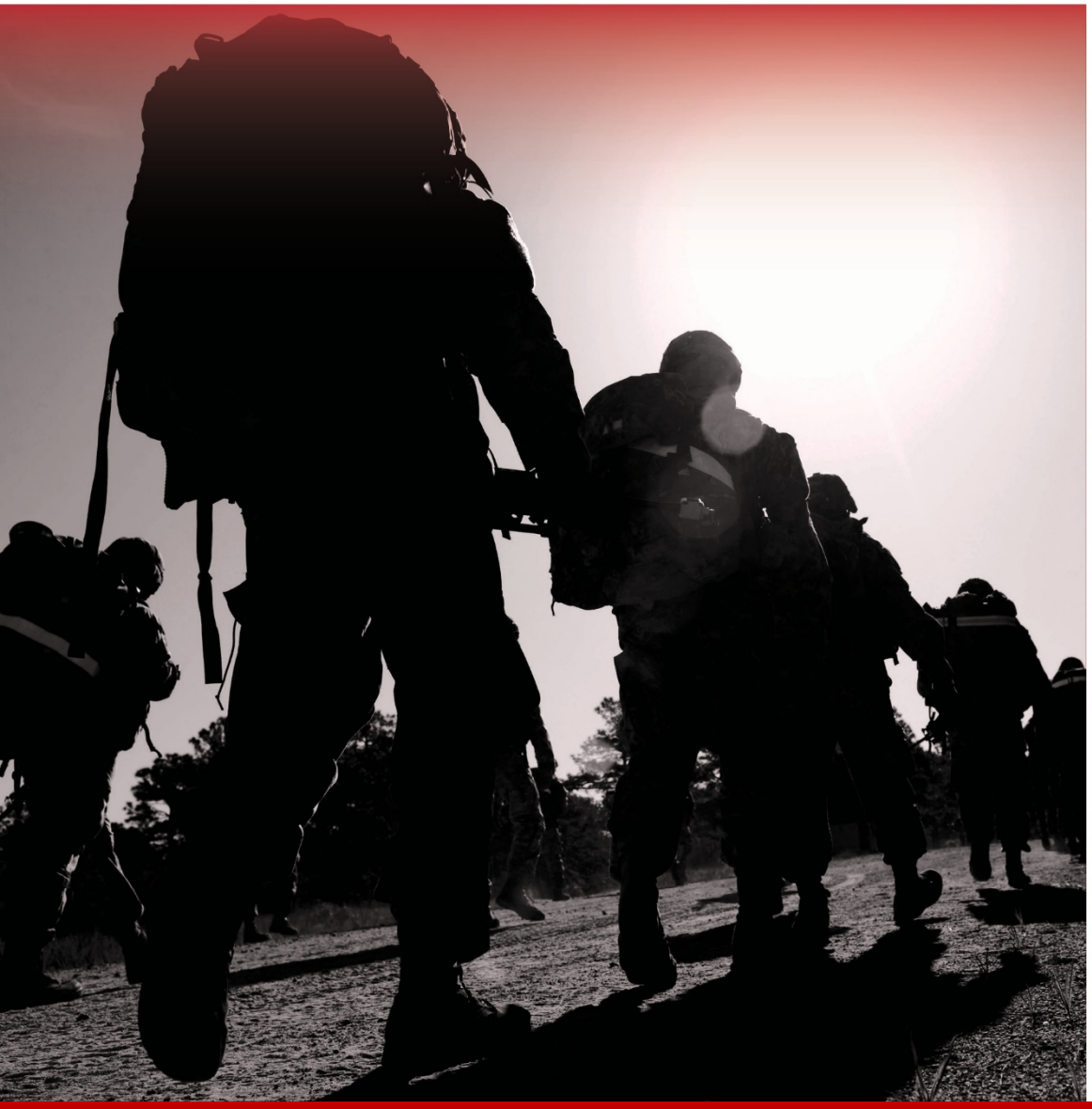
**Congressional Liaison**
703.604.8324

**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



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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