# RESPONSE TO REPORT DODIG-2019-106 PURSUANT TO THE JAMES M. INHOFE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2023, PUB. L. NO. 117-263, SECTION 5274

The Department of Defense Office of Inspector General (DoD OIG) attaches the following response received from specifically identified non-governmental organizations or business entities as required by the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Public Law No. 117-263 § 5274.

The DoD OIG offers no comment and makes no representations, express or implied, of any nature with respect to the matters stated in the attached responses.

Lexmark

Neill Kahle
General Counsel, Americas & Asia-Pacific

Lexmark International, Inc.
740 West New Circle Road
Lexington, Kentucky 40550

Phone: +1-859-232-7892
Fax: +1-859-232-7850
Neill.kahle@lexmark.com

January 20, 2023

The Honorable Robert Storch
Inspector General
Department of Defense
4500 Mark Center Drive
Alexandria, VA 22360-1500
Via Email

Dear Inspector General Storch,

Pursuant to the National Defense Authorization Act (NDAA), Lexmark International Inc. (Lexmark) submits this statement for attachment to the July 26, 2019, Department of Defense Office of the Inspector General (DOD OIG) report titled "*Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items*" (DODIG-2019-106; "Audit/Report"). The Report discusses the vulnerabilities inherent in off-the-shelf information technology equipment and contains a number of recommendations on how the Department of Defense (DOD) can improve its acquisitions practices to better manage the risk posed by these items and refers to Lexmark by name eight times.

This written response to the DOD OIG Audit states formally that Lexmark objects to the statement in the Audit that Lexmark is a "company with connections to Chinese military, nuclear, and cyberespionage programs." According to the Audit, this statement is based on a U.S.-China Economic and Security Review Commission Report (also referred to in the OIG audit as a "Congressional report"); while not disclosed in the OIG's report, the actual source of the statement is a report prepared by Interos (Interos/Interos Report), a private company.

Lexmark further objects to the statement that its printers have known cybersecurity vulnerabilities; this statement is misleading as written because it does not explain the age of these vulnerabilities or that more than half of these cited vulnerabilities had been identified, reported, and addressed in 2014 or earlier and thus relate to older, potentially obsolete printer models.[1]

This letter is necessary because the DOD OIG Audit report's mischaracterization is both misleading and damaging to Lexmark, a U.S. company providing employment to more than 2,000 Americans and a vendor in good standing with the federal government through a National Security Agreement entered into with the DOD and Homeland Security (DHS).

**DOD OIG's Failures**

Lexmark's objections to the Audit are based on several factors, including that the DOD OIG failed to:

- Conduct a thorough review of the Interos Report or the sources upon which it relied;
- Comply fully with its own internal policies and procedures;
- Comply with applicable audit standards;
- Document analysis or review of the evidence supporting its assertions about Lexmark; and
- Offer Lexmark an opportunity to provide additional information and comment on the Audit's conclusions, a reasonable courtesy extended to other corporations as reported in other DOD OIG audit reports.

Interos, a private corporation, authored a report titled: "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology." DOD OIG cites this report as the sole basis for the

[1] The anticipated life expectancy of a laser printer is only about five years.

untrue statement about Lexmark, and it is clear from the OIG Report that the auditors did not understand the underlying Interos Report. For example, while the Interos Report does identify certain firms as presenting a cyberespionage risk, the Interos Report makes no such claim about Lexmark. Although the Interos Report identifies some firms as being connected with China's military or nuclear programs, Lexmark is not one of them.

The Interos Report labels Lexmark as "state-influenced" in its report, presumably because of Lexmark's foreign ownership, but makes no mention of Lexmark's National Security Agreement (NSA) with the DOD and DHS or the annual audits that ensure Lexmark's independence from its investors.

Significantly, the DOD OIG neither contacted nor interviewed anyone at Interos or any of the Interos Report's authors to understand how Interos reached its conclusions. Such outreach would have been particularly useful since the Interos Report itself features an important caveat to its own categorizations on page 14: "Further research would need to be completed to truly understand the comprehensive risk these entities may pose to U.S. ICT [information and communications technology] supply chains." It is also critical to note that Lexmark was not listed as a banned or restricted commercial off-the-shelf (COTS) manufacturer in the DOD OIG Audit.

The Inspector General Act, Government Auditing Standards, and the DOD OIG's own internal policies and procedures require the OIG to maintain information on all evidence relied on in an audit, as well as details about how the auditors analyzed the evidence to determine its relevance, validity, and reliability. The only piece of audit evidence used in support of the incorrect claim about Lexmark's connections was the Interos Report. As acknowledged in writing by DOD OIG, no analysis of this isolated piece of evidence was documented in support of the DOD OIG's conclusion. Moreover, no work papers were prepared to explain the DOD OIG's analysis of the Interos Report or how the auditors came to incorrectly confuse statements made about other firms named in the Interos Report with Lexmark. Additionally, because there were no workpapers addressing the auditors' analysis of the Interos Report, required quality control procedures such as supervisory review of audit conclusions and independent referencing could not have been applied to the misstatements about Lexmark, and the DOD OIG's error was not identified before issuance of the Audit. Surprisingly, the DOD OIG also acknowledged in writing that it failed to assess the evidence individually in the Audit, but instead looked only at the totality of the evidence; a practice which again is inconsistent with applicable audit standards.

Government Auditing Standards emphasize the importance of accuracy and the DOD OIG's Handbook requires an auditor to "exercise reasonable care and observe the principles of serving the public interest." Specifically, the audit standards require the DOD OIG to:

- Assess whether the audit evidence (i.e., the Interos Report) is relevant, valid, and reliable;
- Determine whether enough evidence has been obtained to persuade a knowledgeable person that the findings are reasonable; and
- Document the work performed (analysis) and evidence obtained.

With regard to the statements about Lexmark and its purported connections to Chinese military, nuclear, and cyberespionage programs, DOD OIG failed to meet every one of these requirements. Moreover, DOD OIG did not shield or redact Lexmark's name when it issued the public version of the OIG Audit, even though Lexmark was not the intended focus of the Audit, and DOD OIG made no recommendations or suggestions regarding Lexmark. Instead, the Audit's recommendations were limited to suggested changes to DOD practices.

**Inconsistent Treatment of Private Enterprises at DOD OIG**

Lexmark notes also that DOD OIG treats private businesses in vastly different and apparently arbitrary ways, which creates an appearance of unfairness and a lack of objectivity. DOD OIG's haphazard practices in its treatment of private businesses allow some private enterprises an opportunity to provide input that may impact audit conclusions, while other private businesses are given no opportunity to correct auditors' errors, review draft audit findings, or comment on such findings prior to their release.

For example, DOD OIG policies and procedures do not appear to contain a policy or other guidance about

how to refer to private enterprises and whether to communicate with those same enterprises during the course of an audit. Additionally, DOD OIG's practices differ from audit to audit with regard to identifying private enterprises in publicly issued reports. At times, private entities are identified by name in a publicly issued report (e.g., Audit No. DODIG- 2019-106). Other times, firms are referred to in generalities (e.g., Audit No. DODIG- 2021-080 – "one of the contractors for the Military Health Benefits program did not accurately process health benefit claims.") And finally, some firms are referred to by contract number and other identifying information without publishing the name of the firm (e.g., Audit No. DODIG- 2021-074 – Appendix B includes a schedule with contract number, award date, location, etc.)

In contrast to the DOD OIG's treatment of Lexmark in the Audit, a review of Audit No. DODIG-2019-105, issued on July 23, 2019, is revealing. In that case, the DOD OIG audit team "interviewed chief executive officers, information technology directors … to identify security protocols implemented to protect CUI." (p. 57). Additionally, that audit identified private entities only by coded letter (e.g., Contractor A) and incorporated explanatory information provided by the private entities into the body of the report, e.g., "A Contractor F official stated that it could not encrypt removable media devices because the equipment used with the devices did not support encryption." (p. 19).

In yet another situation, in Audit DODIG-2018-094, contractors were identified by coded letter (e.g., Contractor A), and "The contractors were provided the opportunity to review and comment on relevant portions of the draft report. Comments provided by the contractors were considered in preparing the final report." (p. 33). Notably, this report also included explanations provided by contractors as part of the narrative – "The information technology director at Contractor B stated that instead of implementing technical safeguards to control the use of removable media, it physically controlled CDs by storing them in a locked cabinet." (p. 15).

In Audit No. DODIG-2021-053, issued February 11, 2021, DOD OIG named the specific firms under review but further noted "The contractors were provided the opportunity to review and comment on relevant portions of the draft report, and any comments provided were considered in preparing the final report." (p. 34). Additionally, a two-page Appendix to this same report provided additional context about DOD OIG's conclusion that Moog experienced challenges meeting on-time delivery goals and included details about Moog's corrective actions to improve on-time delivery as well as a section on the progress of Moog's corrective action plan. (pp. 40-41).

In the case of Lexmark, no one from Lexmark was interviewed or contacted about the Audit. Because Lexmark was unaware of the Audit and was given no opportunity to address misstatements or inaccurate conclusions, Lexmark had neither the opportunity to offer corrections nor to provide additional and vital context. Moreover, Lexmark has suffered substantially as a result of these failures.

**CFIUS**

The Committee on Foreign Investment in the United States (CFIUS) was created to balance the U.S. commitment to open investment with the reality that certain investments in the U.S. from foreign persons, particularly those from competitor or adversarial nations can present risks to U.S. national security. As a result, the United States maintains a robust foreign investment review process to identify and address such risks.

Lexmark has and continues to comply fully with its CFIUS-mandated obligations. In a letter dated September 29, 2016, CFIUS stated that there are 'no unresolved national security concerns" with the proposed acquisition of Lexmark International Inc. (Lexmark) by a consortium of foreign investors. Indeed, as a precondition to CFIUS' clearance of the proposed acquisition, CFIUS required that Lexmark and the consortium of foreign investors enter into a National Security Agreement with the DOD and DHS.

As is well established, after its acquisition by investors including Ninestar Corp, PAG Asia Capital, and Legend Capital, Lexmark remained an independent U.S. company. CFIUS approved the transaction after conducting a thorough review to ensure that U.S. national security interests were not at risk. The National Security Agreement entered into by Lexmark and its investors includes the following key provisions:

- Requires that Lexmark remain a U.S. company with a Board of Directors made up entirely of

U.S. citizens that operate independently of investors.

- Restricts the interaction between Lexmark and its investors and prohibits Lexmark from sharing with its investors any information about Lexmark, and its U.S. customers, including their identities, their IT environments, their product purchases, warranty information, and customer service or support information.
- Prohibits joint research or development activities between Lexmark and its investors and prohibits Lexmark from sharing technical details with its investors, including data related to source code development, imaging, installation, firmware development, hardware design, hardware development, software testing, firmware compilation, software compilation, and firmware installation.
- Requires that all Lexmark source codes be managed, stored, and maintained in the U.S., and any device that is custom configured for a U.S. customer must be configured in the U.S.
- All level 3 customer service for products installed in the U.S. is required to be performed by U.S. residents and every Lexmark third-party service provider performing customer service or warranty services in the U.S. must be approved by the DOD and DHS.

Lexmark's distinguished board of directors, which includes three former cabinet members and a Nobel prize winner, is elected by five Proxy Holders who stand in the place of our investors and serve as directors themselves. As set forth in the National Security Agreement, these Proxy Holders must:

- Remain independent of the company's investors;
- Be resident U.S. citizens;
- Have no prior contractual, financial, or employment relationship with our investors; and
- Be eligible to hold a U.S. personnel security clearance and be approved in advance by CFIUS.

The National Security Agreement's requirements also prohibit Lexmark's investors from having access to:

- The Lexmark network;
- Source code of any kind; and
- U.S. customer information.

Moreover, the National Security Agreement prohibits Lexmark from selling or otherwise transferring assets or services to its investors without approval in advance by the DOD and DHS, two U.S. defense agencies designated in the National Security Agreement as the CFIUS Monitoring Agencies. Lexmark investors are prohibited from entering any Lexmark facility unless approved and documented in advance by Lexmark's Security Officer and a Lexmark Board Member.

Lexmark is audited annually by its independent, government approved Security Monitor, Deloitte, and by an internal compliance team to ensure adherence to the controls that have been implemented to prevent breach of its National Security Agreement. Both audit teams report all findings directly to the CFIUS Monitoring Agencies, as well as to the company's board of directors. Every annual audit conducted since the acquisition has found Lexmark to be substantially compliant with the terms of the NSA.

**National Vulnerabilities Database (NVD)**

Lexmark has and continues to be committed to upholding the highest cybersecurity standards to ensure our products and customer data are safeguarded against potential threats. Security is an integral design and engineering component embedded into all Lexmark products, tools, and services and Lexmark's advanced security capabilities help minimize threats and vulnerabilities.

Lexmark meets the most stringent industry and government security standards including Common Criteria and Federal Information Processing Standard (FIPS). The Lexmark security ecosystem is designed to overcome the most complex data protection challenges. The DOD OIG Audit assertion that Lexmark printers have "known cybersecurity vulnerabilities" is misleading and is tied to the blog from Threat Post cited in the Interos Report. This assertion, taken out of context, completely ignores that Lexmark has a responsible vulnerability management process and works to quickly identify, patch, and disclose any potential threats rapidly to protect its products and customers.

The National Vulnerabilities Database (NVD) is a repository of standards-based vulnerability management data. In essence, it enables the automation of vulnerability management, security measurement, and compliance and includes databases of security checklist references including security related software flaws. The NVD does not actively perform vulnerability testing; instead, it relies on security-conscious vendors and others to provide information voluntarily. Lexmark's participation in the NVD is a net positive as it results in transparency and ultimately more secure products. Unfortunately, the Audit's reference to "known cybersecurity vulnerabilities" effectively punishes Lexmark for efforts to act as a responsible product manufacturer in reporting vulnerabilities, an industry best practice, to the NVD. In doing so, the Audit effectively discourages participation by vendors with the NVD.

Moreover, the Audit, instead of providing necessary context regarding cited vulnerabilities instead stated only that Lexmark has "known cybersecurity vulnerabilities." To put this in perspective, a search of the 132,000 different vulnerabilities listed in the NVD during the relevant period reveals that at least four of Lexmark's competitors had more than 20 vulnerabilities listed in the database over the same period.

Notably, each of the 20 vulnerabilities attributed to Lexmark had already been identified, reported, and addressed by Lexmark at the time of the Audit. In addition, most of the identified vulnerabilities related to older printer models and most, if not all, were likely obsolete at the time of the Audit. This would have been readily apparent to the DOD OIG had it made any effort whatsoever to contact Lexmark about the NVD or about the Audit prior to its release.

**Conclusion**

Lexmark agrees with the broad conclusions of the Audit and supports its key recommendations that DOD 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. However, Lexmark also categorically disputes the Audit's unsupported and inaccurate characterization of Lexmark as a "company with connections to Chinese military, nuclear, and cyberespionage programs." Lexmark remains a U.S. company providing employment to more than 2,000 Americans and a vendor in good standing with the federal government through a National Security Agreement entered into with the Departments of Defense and Homeland Security.

Should you have any questions regarding this response, please do not hesitate to contact Patrick Brewer, Lexmark's director of worldwide government affairs, at patrick.brewer@lexmark.com or 859.232.2303.

Yours sincerely,