RESPONSES 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 responses 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.

Because these comments were submitted more than 30 days after the enactment of Public Law No. 117-263, the retroactive provisions of § 5274 (b) are inapplicable. We are under no obligation to attach these comments to the report. However, because we are attaching other comments that were submitted in a timely manner under § 5274 (b), we are voluntarily attaching these comments in the interest of transparency.

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.

Lenovo.com

8001 Development Drive
Morrisville, NC 27560

March 10, 2023

The Honorable Robert Storch
Inspector General
U.S. Department of Defense
4800 Mark Center Drive, Suite 15G27
Alexandria, VA 22350

VIA Email

Dear Inspector General Storch:

I am writing on behalf of Lenovo Group Ltd. to submit the attached response to Department of Defense Inspector General (DOD IG) Report #DODIG-2019-106.

The purpose of this response is to correct, clarify and provide additional context regarding specific references to Lenovo in that report, as authorized by Section 5274 of Public Law 117-263. I understand this law also requires that such a response be attached to the original report and that the version of the report on your website be similarly updated.

Lenovo was not notified by your office of the opportunity provided by Public Law 117-263 to submit a response to Report #DODIG-2019-106, which was published on July 26, 2019. I therefore request that you fulfill the intent of Section 5274 to ensure that businesses can respond to public assertions about them. Making Lenovo's response available to the public would also be in keeping with your office's commitment to integrity, independence, and excellence.

I appreciate your attention to this important matter and look forward to your response.

Very truly yours,

Laura Quatela
Senior Vice President
Chief Legal & Corporate Responsibility Officer

Attachment: Lenovo Response to U.S. Department of Defense Inspector General Report, DODIG-2019-106, March 10, 2023

cc: Steven Stebbins
Michael Zola

Lenovo.com

8001 Development Drive
Morrisville, NC 27560

LENOVO RESPONSE TO U.S. DEPARTMENT OF DEFENSE INSPECTOR GENERAL REPORT, DODIG-2019-106

March 10, 2023

The following is a response by Lenovo Group Ltd. ("Lenovo") to Department of Defense Inspector General (DOD IG) report #DODIG-2019-106, pursuant to Section 5274 of Public Law 117-263. The purpose of this response is to correct, clarify and provide additional context regarding specific references to Lenovo in the report.

To clarify the report's characterization, Lenovo is a global company that is listed on the Hong Kong Stock Exchange and has headquarters in both the United States and China. Lenovo's U.S. operations are headquartered in Morrisville, North Carolina, where it employs more than 5,000 individuals, in addition to over 1,000 in other U.S. states, including corporate offices in California, Illinois, and Washington State. As a public company, Lenovo is subject to global corporate governance requirements that include rigorous reporting, disclosure and financial transparency rules. Lenovo's leadership team is comprised of several U.S. citizens, including its Chief Legal Officer, its Chief Security Officer, its Chief Information Security Officer, the Senior Vice President of its International Sales Organization, and the Executive Vice President of its Infrastructure Solutions Group.

I. DOD IG Report Assertions and Omissions

The stated purpose of the 2019 DOD IG report was to audit the department's management of cybersecurity risks when purchasing commercial off-the-shelf (COTS) information technology products. The report recommended that agencies develop a risk-based approach for the purchase of these items, which Lenovo fully supports as an industry-wide best practice.

Contrary to mischaracterizations since the publication of this report, it specifically stated that Lenovo products have not been banned by DOD and it did not propose such a ban. However, the report did raise certain concerns regarding Lenovo products but either failed to substantiate them, did not acknowledge that they were subsequently resolved, or neglected to explain that product vulnerabilities are an inherent challenge that all vendors, including Lenovo's U.S. competitors, work to resolve on a continuous basis. The context for and resolution of the report's references to Lenovo are addressed below.

The report failed to note that beginning in 2005, Lenovo successfully completed five national security reviews by the interagency U.S. Committee on Foreign Investment in the United States (CFIUS), and that the company has complied fully with post-review third party audits and other oversight requirements. The report also declined to acknowledge that Lenovo has been a Government Services Administration-approved vendor of products for the U.S. Government since 2005 and,

through its listing on the GSA's Multiple Award Schedule, offers products to federal, state, and local government agencies at pre-negotiated prices.

II. Specific References to Lenovo

The report asserted that certain U.S. Government agencies had made decisions or issued warnings in the past about the cybersecurity risks of using Lenovo products, citing only three specific instances that are addressed below.

- **Issue 1**: The report stated that "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."
- **Response**: Lenovo computers were not in 2006 and are not today manufactured with hidden hardware or software used for cyberespionage, and Lenovo is unaware of any credible reports to the contrary, including those referenced in the DOD IG report. In addition, just months before this reported action, CFIUS reviewed and approved Lenovo's acquisition of the personal computer business of IBM, the source of the equipment that Lenovo subsequently sold to the State Department. In addition, the State Department has continued to purchase Lenovo personal computers since 2006.

- **Issue 2**: The report stated that in 2015, the Department of Homeland Security issued cybersecurity warnings related to pre-installed spyware and other cybersecurity vulnerabilities identified in Lenovo computers.
- **Response**: In late 2014 and early 2015, Lenovo installed a third-party component – the VisualDiscovery "shopping assistant" software manufactured by the Israeli company Superfish – on limited personal computer models with the intent of enhancing consumers' online shopping experience. When researchers discovered a vulnerability in this software, Lenovo immediately stopped installing it. The company also published a security advisory, provided customers with an automated tool to remove the software and all associated certificates, and is not aware of any instance of the vulnerability having been exploited to access user information.

  Similar vulnerabilities caused by third-party software were found in products of other personal computer manufacturers during this same period.

  In addition to helping customers remove this software, Lenovo agreed to biennial independent assessments and other requirements established by the U.S. Federal Trade Commission, measures that our competitors' products with similar vulnerabilities did not undergo.

- **Issue 3**: The report stated that in 2016, the Joint Chiefs of Staff Intelligence Directorate issued a warning that Lenovo computers and handheld devices could introduce compromised hardware into the Department of Defense supply chain.
- **Response**: Lenovo is not aware of any such warning and we remain a GSA-approved vendor to DOD and other Federal agencies. Lenovo strives to create products that meet or exceed industry security standards. At the forefront of this commitment, Lenovo has established a governance structure to drive security across products and services development. Our Lenovo Secure Development Lifecycle (LSDL), adopted from Microsoft, SAFECode Fundamental

Practices for Secure Software Development, and ISO 27034, guides security efforts for products and services throughout our business units to reduce risk. The cornerstone of the LSDL process is a Security Review Board (SRB) led by executives in Morrisville, North Carolina, that engages with products and services development teams throughout the entire product lifecycle. The design is reviewed and approved by the SRB early in the development cycle. When the product is nearing release, the product itself is tested, reviewed again, and approved. The SRB decides what elements need further review, testing, and/or remediation, and holds final veto power over their release to the market. Ultimately, the SRB structure enables Lenovo to standardize company practices around our LSDL to ensure that security is built in from the start.

III. Additional Context Regarding ICT Vulnerabilities

The DOD IG report made general references to vulnerabilities associated with products made by Lenovo and other companies. It failed, however, to acknowledge that all information technology products and services contend with vulnerabilities of varying degrees of severity, regardless of manufacturer or country of origin. To address this industry-wide challenge, Lenovo has robust processes in place to ensure that vulnerabilities discovered in our products are addressed in a timely manner through patches, code updates, and/or other mitigating actions.

Lenovo's security leadership is comprised of U.S. and UK nationals who manage product security teams that proactively identify and repair vulnerabilities in our products as part of our LSDL process, which includes regular audits by customers and third parties approved by the U.S. Government. Lenovo also maintains a dedicated, U.S.-based Product Security Incident Response Team (PSIRT) to receive vulnerability reports from researchers, industry partners, and customers. In response to any report, Lenovo's PSIRT works with development teams and industry suppliers on an applicable repair or mitigation, documents the vulnerability and patch, and reports this to the National Vulnerability Database (nvd.nist.gov). This U.S. Government database tracks security vulnerabilities in products manufactured by Microsoft, Intel, Apple, Dell, Lenovo, and other global companies. For example, during the four-month period starting November 1, 2022, the National Vulnerability Database recorded 18 vulnerabilities in Lenovo products, 86 in Cisco products, 91 in Dell products, 155 in Apple products, 156 in IBM products, 312 in Microsoft products and 474 in Intel products.

To ensure supply chain security, Lenovo carefully evaluates, qualifies and periodically audits all suppliers. We also utilize the Intel® Transparent Supply Chain, which secures devices from manufacturing through transport, delivery and setup by our customers.

IV. Lenovo Support for Additional Security Oversight

The DOD IG report recommended that DOD develop a risk-based approach to prioritize commercial off-the-shelf products for further evaluation and testing. Lenovo welcomes an approach that applies to all manufacturers and reflects best practices for this industry. We would also welcome further engagement with DOD on these matters, including a full review of our product security programs and security assessments of Lenovo products.