
August 31, 2016

Daryl Cromer
Chief Product Security Officer
Lenovo
1009 Think Place
Morrisville, NC 27560

**RE: Letter of Attestation for Supply Chain Security Program**

Dear Mr. Cromer:

As requested, Chain Security is providing Lenovo with this letter of attestation to attest that Chain Security has reviewed certain aspects of Lenovo's product security program ("Program"). We describe herein our findings and conclusions based on this review.

Chain Security is an outside advisory firm retained by Lenovo. We anticipate that Lenovo will provide this letter to customers and interested parties, and we are happy to be a resource for such parties who wish to get our third-party view on the state of Lenovo's Program. (An overview of Chain Security's qualifications and expertise can be found in Attachment A to this letter.) We anticipate that customers may have questions or want more detail regarding the high-level descriptions contained herein, and Chain Security will support Lenovo to provide those additional details and descriptions as needed.

## EXECUTIVE SUMMARY

Chain Security has gathered information from Lenovo through multiple meetings, interviews and telephone conversations with Lenovo officers and employees, as well as from review of documentation provided by Lenovo. Chain Security has directed the information gathering process and made specific requests to Lenovo for information that relates to Lenovo's Program. This information gathering process has been guided by Chain Security's expertise and experience in security-related matters, stemming from service in U.S. Government positions and senior management and engineering positions in the commercial sector, as well as strong engineering and product development expertise. We assess that Lenovo has been cooperative and has readily provided the requested information.

Our inquiry has focused on the following components of the Program: (1) Lenovo's corporate commitment to the Program and delegation of authority for the Program ("Corporate Governance"); (2) integration of the Program into Lenovo's operations and processes generally ("Security Processes"); (3) security related to Lenovo's component and subcomponent suppliers (i.e., traditional supply chain) and the implementation of Lenovo's *Trusted Supplier Program* ("Trusted Supplier Program"); and (4) an intensive initiative to

scrutinize the security of pre-loaded software associated with the latest release of the Windows 10 operating system, which runs on Lenovo products ("Windows 10 Pre-Load").

The following is an executive summary of our findings and conclusions regarding these four components of the Program:

**Corporate Governance**

- Lenovo's CEO has directed each business unit to implement the Program, with support from the Lenovo Product Security Office ("PSO"), across Lenovo's global operations, under the direction of the Chief Product Security Officer ("CPSO"). The CPSO as well as the PSO and all of its employees are located in Morrisville, North Carolina, but the PSO draws on company-wide resources.
- Lenovo's CEO has delegated full authority for the Program to the CPSO.
- The CPSO and the PSO are actively promulgating and implementing policies and procedures for components of the Program and are training Lenovo employees on the Program.

**Security Processes**

- Under the Program, Lenovo implements security requirements through its Offering Delivery Teams ("ODT"), which are responsible for the design, development and production of Lenovo products.
- Each ODT must develop and comply with a Product Security Profile for each product they produce. The Product Security Profile includes each component of the Program in its requirements.
- ODT leads are ultimately responsible for security compliance and are assisted by key ODT team members, and the PSO. ODTs must report to the PSO at key product development process gates or checkpoints in the process regarding compliance with their Product Security Profile requirements.
- Lenovo has provided training on the Program and the requirement for using Product Security Profiles for all ODT leads for the following product lines: ThinkPad, ThinkStation, ThinkCentre, Lenovo Notebook, Desktop, and Servers (ThinkServer and System x).
- The CPSO has authority to stop shipment on any Lenovo product that has not met Program requirements.

**Trusted Supplier Program**

- Lenovo has developed a Trusted Supplier Program, whereby every supplier of "Intelligent Components" that are included in Lenovo products must be vetted and approved from a security perspective.
- The PSO and procurement personnel submit security questionnaires to each prospective supplier. The suppliers must provide accurate information to Lenovo on

matters such as the location and ownership of the supplier and the supplier's internal security practices and procedures.

- Lenovo has developed contractual language for suppliers that requires suppliers to warrant and represent that the information that the supplier has provided is accurate.
- The PSO conducts a risk analysis on each supplier using the information provided. Any supplier that receives a high risk rating is excluded from Lenovo's Trusted Supplier List unless the CPSO (or the CPSO's designee) grants an exception.
- The ODTs can only source components from suppliers on the Trusted Supplier List.

**Windows 10 Pre-Load**

- In February 2015, Lenovo implemented a process to conduct a security review of every software application that was to be included as pre-loaded software in connection with the release of products containing the Windows 10 operating system ("Windows 10 Pre-Loads"), which reached the market in late summer 2015. This process was implemented to fulfil the "Cleaner and Safer" initiative that was publically announced. (http://news.lenovo.com/news-releases/lenovos-promise-for-cleaner-safer-pc.htm)
- This Windows 10 security review and pre-load vetting process ("Win10 Process") was established by and functions under the direction of the CPSO, with support from the PSO. The CPSO established a software security review board ("SSRB") consisting of personnel from Lenovo business units that produce Lenovo Notebooks, Desktops, ThinkPads, ThinkCentres and ThinkStations.
- Lenovo engaged two prominent third party software security firms to provide third party reviews.
- Through the fiscal year ending March 31, 2016, Lenovo had subjected over 430 software internal and third-party applications to the Win10 Process. Firmware was outside the scope of the review. As part of the process, Lenovo conducts security reviews including the use of internal and external tools and sends software applications with high-level security vulnerabilities to 3rd party security groups for further review. All high and medium risk issues identified were remediated as part of the process. If any application's risk could not be remediated, then the application was removed from the preload or very limited exceptions were approved.
- Under the direction of the CPSO and the PSO, Lenovo has managed the process of screening applications for its final "golden" pre-load software images (i.e., the image sent to manufacturing to be loaded onto hard drives) to include only applications that were approved in the Win10 Process.

We have also reviewed other components of the Program that are still in development. For example, Lenovo is in the process of improving security for Lenovo's firmware for its basic

input/output system (BIOS) and unified extensible firmware interface (UEFI) ("BIOS Security"). Lenovo also intends to pursue additional security requirements governing the full software lifecycle for all software loaded on Lenovo products, beyond the Windows 10 Pre-Load effort ("Software Lifecycle"). Chain Security will re-issue this letter of attestation with updates as dictated by Lenovo's progress on programs such as BIOS Security and the Software Lifecycle.

## SCOPE OF REVIEW

As of the date of this letter, Chain Security has conducted in-depth interviews with a wide variety of Lenovo personnel, including officers and managers and their direct reports, all of whom are currently located at Lenovo's North American headquarters in Morrisville, North Carolina. These include (but are not limited to):

Chief Product Security Officer
Chief Quality Officer
Chief Security Officer
Director of Security Architecture
Director of the Product Security Office
Senior Program Manager in the Product Security Office
Program Manager for Secure Development
Program Manager for Supply Chain Security
Global Commodity Managers
Offering Delivery Team Leads for specific products
Director of Software Development/Pre-Load Manager
SSRB lead

We have also reviewed documents provided by Lenovo and have had access to and viewed internal Lenovo networks and databases. While we believe we have performed sufficient diligence and data gathering to provide this letter and to reach the findings and conclusions herein, Chain Security has not independently verified every fact provided by Lenovo. Chain Security and Lenovo have been engaged in developing and implementing the Program for over two years and contemplate an ongoing review and enhancement of Lenovo processes over the coming months.

## PARAMETERS OF THE ATTESTATION

Chain Security has requested and reviewed information from Lenovo regarding its product development and supply chain processes in connection with the Program, with a focus on the security of those processes. We are not providing in this letter a full description of Lenovo's processes nor do we attempt to detail every fact that we have gathered during the review process, but instead are attesting to and recounting only those high-level facts and

conclusions that, in our professional judgment, are likely to interest Lenovo customers, including the U.S. Government, who are focused on the security of Lenovo's supply chain and development processes. As noted above, we stand ready to answer questions and provide further details as requested by relevant third parties.

Chain Security applauds Lenovo's focus on supply chain and product development security. We encourage a comparison of Lenovo to other vendors and competitors (including U.S.-based companies) on supply chain and product development security matters. We assess that Lenovo is likely ahead of the industry in terms of its focus on and commitment to these issues.

## KEY FINDINGS

The following is a summary of Chain Security's key findings regarding the Program. As noted above, we are recounting herein only a summary of facts that are relevant to our findings:

### Corporate Governance

In 2014, Lenovo created its PSO to develop and implement the Program, which is intended to be a broad product security program that spans across Lenovo product lines. The PSO is based in and staffed by personnel in Lenovo's North American headquarters in Morrisville, North Carolina. The PSO works with and draws upon the expertise and resources of product teams throughout Lenovo's global operations.

The PSO is under the direct supervision of Lenovo's CPSO. In an internal policy document issued on February 2, 2016 (Corporate Policy # 21 – Lenovo Product Security Policy), which is attached hereto as Attachment B ("February 2016 Policy"), Lenovo's Chief Executive Officer granted the CPSO full corporate authority, with the resources of the PSO, to implement and be responsible for product security across Lenovo's global operations (i.e., to implement the Program). The February 2016 Policy states that "[a]ll Lenovo employees and stakeholders are expected to comply with the Product Security Program, and to be responsive to the Program requirements." The Policy also states that Lenovo "expect[s] Partners and suppliers to make commitments in support of the Security Program as a condition of doing business with [Lenovo]." This Policy has been made available on internal Lenovo systems to Lenovo employees and currently governs Lenovo's global operations.

On August 3, 2016, Lenovo's Chief Executive Officer issued a revised version of Corporate Policy # 21 – Lenovo Product Security Policy, which is attached hereto as Attachment C ("August 2016 Policy"), following corporate organizational changes. The August 2016 Policy reflects the same commitment to the Product Security Program as indicated in the February

2016 Policy and continues to place responsibility for the Program in the CPSO. Lenovo anticipates that the August 2016 Policy will be publicly available through Lenovo's company website. The website is currently being revised and updated. Once the August 2016 Policy is posted on the website, it will replace the February 2016 Policy.

Building on the February 2016 Policy (and reiterated by the August 2016 Policy), in early August 2016 the CPSO issued a Lenovo-wide policy regarding implementation of the Program ("Program Policy"), which is attached hereto as Attachment D. The Program Policy has been made available to all Lenovo employees and indicates that all Lenovo employees are required to comply with the policies as a binding corporate policy. The Program Policy states that "[t]he CPSO (with the support of the Product Security Office) has authority and responsibility for ensuring full implementation of the Product Security Program."

The Program Policy indicates that the Program itself will include the following specific components, each of which will be governed by a component or program policy that will outline specific requirements:

- Product Development, which includes Platform Development and Secure Software Development (Lenovo Secure Development Lifecycle, or LSDL)
- Product Security Governance through the Offering Development Team (ODT), which includes Security Responsibilities of all ODT members and Integration into the Integrated Offering Delivery (IOD) process
- Supply Chain, which includes the Trusted Supplier Program, the Trusted Supplier List, Parts Shipment, Manufacturing, and Finished Goods Shipping
- Product Security Incident Response Team (PSIRT), which includes Organization and Management System and Incident Information

The PSO has implemented a Lenovo-wide training program, primarily through online training modules, to educate Lenovo employees on their obligations under the Program and on supply chain and product security matters generally. As of the date of this letter, four basic training courses have been published by the PSO, plus an introduction into Lenovo Secure Development Lifecycle for software, as well as five core software courses from a 3rd party. Additional advanced classes are also available. As of May 3, 2016, Lenovo employees have completed over 9,400 courses and have passed tests at the end of each course. Lenovo is maintaining records of all courses completed by individual employees.

**Security Processes**

Lenovo develops products through an Integrated Offering Development process ("IOD"), where all sources and disciplines needed to take a product all the way from marketing and customer requirements to a finished and deployed product work as an integrated team through

the entire product lifecycle process. At the root of the IOD process is the platform Offering Delivery Team ("ODT").

Every product produced by Lenovo has its genesis and is managed by a product-specific ODT. Each discipline needed for completion of the product is represented on the ODT. Each ODT has a team "lead" who is responsible for managing the team's processes. The ODT lead reports up to the senior managers of specific Lenovo business units and brand teams (e.g., Lenovo's Data Center Product Group, which produces Lenovo servers, or the PC and Smart Device Business Group, which produces Lenovo ThinkPads and PCs). There are approximately 100 ODTs operating within Lenovo at any given time. For example, for ThinkPads, there are nine ODT leads, all of whom report to an ODT manager within the Think Business Group—four in Morrisville, North Carolina; four in China; and one in Japan. There are approximately 30 ODTs working on server products.

The ODT process begins with a Marketing Requirements Document ("MRD"), an initial and detailed Offering Definition (i.e., the features and functionality that will be included in the product), and a source plan with a key components list which is ultimately translated into a bill of materials ("Source Plan"). These documents together constitute the full set of "requirements" which must be met in order to design, develop and produce the product.

Under the Program, the ODT now plays a pivotal role in security of each product. In a policy document entitled "Integration of Product Security Within The IOD Process," issued in August 2016 by the PSO, under the authority of the CPSO and published to Lenovo's ODTs ("Security Process Policy"), the ODT for each product must create a Product Security Profile ("Profile"). The Profile lists every security requirement of the Program that must be followed and/or included in the product itself as a condition of the product being manufactured and sold to customers. The ODT lead is ultimately responsible for ensuring that each security requirement in the Product Security Profile is met, or provide justification on why it cannot be met.

The ODT leads for the following product lines have undergone training regarding the Security Process Policy and the requirement for using Profiles to check-point security-related matters: ThinkPad, ThinkStation, ThinkCentre, Lenovo Notebook, Desktop, and Servers (ThinkServer and System x).

Each platform ODT includes a Software representative who is the interface into all software activity. The software rep interfaces with the various Software ODT's, from which software applications are developed and/or provided for the system. Each software application has a Software Architect, who will work with the PSO to ensure applications go through the review process. When an application is approved, it can be added to the list of approved software for a platform. This list is a key part to the Product Security Profile for the new

system. The PSO provides resources and guidance/advice to the ODT as needed to help it meet the security requirements.

At defined product development gates or checkpoints through the ODT process, the ODT must update the management team (stakeholders) regarding the Product Security Profile. The key checkpoints are: Concept Exit (preliminary Profile), Plan Exit (committed Profile), and System Integration Test (SIT) Exit (actual Profile). The result of these checkpoints is that before the product can move into manufacturing and finally be released to customers, the ODT lead must certify to the CPSO and the PSO that all requirements of the Profile have been met. The CPSO has authority under the Program, delegated from the CEO, to stop shipment on any product that has not met the Program requirements and fulfilled every element of the Profile for that product. ODT leads can petition the CPSO (via the PSO) to modify or waive a particular Program/Profile requirement for a particular product if there is a compelling commercial need to do so. The CPSO has ultimate discretion and authority whether to grant a waiver or exception.

Pursuant to the Security Process Policy, each product Profile must include at least the following security elements. Additional security elements of the Program will be added to Profiles as Lenovo's implementation of the Program continues to mature:

- As reflected in the MRD for the product, any security-related functionality required by customers (e.g., biometric security controls, custom software image), as well as legal/regulatory requirements (e.g., TAA compliance)
- Only intelligent components (hardware and software) from vendors on the "Trusted Supplier List," which results from the Trusted Supplier Program (see discussion below), are included in the Source Plan (e.g., no non-approved vendor is allowed to provide any intelligent component for the product)
- Long term service and support plans that take into account security requirements (e.g., geography-based service teams)
- Signing of BIOS or UEFI manifests by the PSO[1]
- Software applications that have been cleared through the Windows 10 Pre-Load process (see discussion below) are pre-loaded on the product

As of the date of this letter, every ODT within Lenovo for the platforms indicated above has been informed that he/she is required to meet Profile requirements as a condition of offering any product to customers.

[1] The BIOS Security process is a component of the Program that is continuing to mature as of the date of this letter of attestation. Future versions of this letter will address the BIOS Security process in further detail.

ODT leads who operate out of Lenovo's North Carolina facilities have reported to Chain Security that they are in fact implementing Profiles (as required by the Program) and are interacting with the PSO to ensure security requirements are met.

The CPSO has reported stopping shipment on at least one product because Profile requirements were not met.

**Trusted Supplier Program**

As part of Lenovo's IOD process for developing products, engineering teams on each ODT create a Source Plan that identifies all components to be included in the ultimate bill of materials ("BOM"). In addition, the ODT must identify all software pre-loads that will be included on the product at the time of sale. The Source Plan identifies not only specific components, but also potential suppliers for the components.

Once suppliers have been identified, Lenovo's Global Commodity Managers ("GCMs") must negotiate and enter into supply contracts with the suppliers. In some cases, Lenovo may already have an existing relationship with the supplier. In other cases, Lenovo must forge a new supply relationship. Lenovo and the supplier will typically enter into a supply agreement, which is negotiated by a GCM.

Lenovo has historically had an approval process for identifying and qualifying suppliers based on quality, performance and price. Under the Program, Lenovo has now added security requirements to the supplier qualification process. In a policy document entitled "Trusted Supplier Program," approved by the CSPO on March 15, 2016 ("TSP"), the PSO has implemented policies and procedures to qualify suppliers for inclusion on the Trusted Supplier List ("TSL").

In addition to the TSP being part of the Program, as indicated in the CEO's policy document and in the CPSO's Security Policy, the TSP fulfills a requirement imposed in the CFIUS Agreement in connection with the purchase of IBM's x86 server business, specifically Section 8 of the Agreement.

As indicated above, under the Security Policy and in connection with security requirements on the Profile for each product, ODT leads are prohibited from using any supplier not included on the TSL. ODT team members who have identified a supplier as part of the Source Plan must submit proposed suppliers to the PSO for vetting and inclusion on the TSL.

The TSP documentation has been provided to the ODT leads within Lenovo as well as the GCMs for the following product lines: System X, ThinkServer, Notebooks, Desktop, Thinkpad, ThinkCentre, and ThinkStation. The TSP and supporting materials (described more

fully below) are being translated into Chinese for use by China-based GCMs and ODTs. One of the training sessions made available to Lenovo employees regarding the Program (see discussion above) covers the TSP and the supplier qualification process for inclusion on the TSL.

The PSO is coordinating with managers within the procurement organization who have responsibility for GCMs to ensure that GCMs are implementing the TSP properly. There are currently two such managers—one in Lenovo's North Carolina facility and one in China. The PSO tracks the performance of GCMs regarding the TSP process and gives tracking data to the managers. The PSO also regularly updates the CPSO on tracking suppliers who are moving through the process of inclusion on the TSL.

The following is a description of the TSP and how suppliers are included on the TSL, as well as how ODT's use the TSL when creating Source Plans and fulfilling Profile requirements:

Under the TSP, the TSL is limited to suppliers who are providing "Intelligent Components" for Lenovo products. The TSP defines Intelligent Components as "(a) any hardware, software or firmware executable on any microprocessor, (b) the microprocessor itself, (c) any semiconductor device that has processing ability (d) any device that has internal memory, (e) any component or device that performs a communication function, and (f) any hardware, firmware or software (including operating systems) integrated into or installed on an Intelligent Component." Intelligent Components can include components, sub-assemblies, whole product assemblies, firmware (including in any component or sub-assembly), and software installed onto the products.

Although both hardware and software components qualify as Intelligent Components, as of the date of this letter of attestation, Lenovo has only implemented the TSP in connection with hardware (including firmware). As Lenovo's TSP matures, software suppliers will be added (beyond the processes surrounding Windows 10 Pre-Load, as discussed below).

Each supplier of an Intelligent Component is issued a security questionnaire that has been developed by the PSO. The questionnaire seeks disclosures from suppliers on a wide range of security-related questions, including but not limited to location and ownership of the suppliers, security-related incidents, internal security controls within the suppliers' operations, and visibility and traceability into the suppliers' own supply chains. The questionnaires are provided to the suppliers by the GCMs. The GCMs gather the completed questionnaires and forward them to the PSO for review and analysis.

The PSO uses a risk analysis model for assessing the information provided on the security questionnaires. The risk model assesses (1) threat posed by the supplier, (2) vulnerability associated with the supplier's product/component/sub-assembly, (3) likelihood of exploitation, and (4) impact and consequences of exploitation. Each element of the risk model

is scored as “no threat/vulnerability,” “low,” “medium” or “high.” The elements are combined to create an overall risk score. A supplier that receives an overall “low” risk is added to the TSL. A supplier that receives an overall “medium” risk is added to the TSL but is flagged with a caution, so that the ODT and ultimately the PSO are aware that there may be security issues to address. The PSO will work with the GCM to urge the supplier to improve its security posture. A supplier that receives an overall “high” risk cannot be included on the TSL unless there are compelling business reasons to do so and the CPSO specifically authorizes the inclusion, after assessing the overall risk profile of the supplier.

For any supplier that qualifies for inclusion on the TSL, Lenovo (via the GCM) negotiates a supplier agreement. The PSO has developed standard contractual language to be used by the GCM in this process. The supplier contract requires the supplier to warrant and represent that the security-related information on the questionnaire is correct. The supplier contract also gives Lenovo the right to conduct security audits of the supplier. For long-standing supplier contracts that existed before the TSP, the PSO and GCMs are seeking to amend existing supplier contracts to include the security-specific provisions.

The TSL is maintained by the PSO as a “living document” that reflects ongoing vetting of suppliers.

The PSO provides each ODT with access to the current TSL, enabling the ODTs to review the Source Plan to ensure that every Intelligent Component in each product’s BOM is being supplied by a supplier on the TSL. The comparison against the TSL by the ODT is done in coordination with the PSO, which serves as a resource to the ODT.

The PSO retains a repository of all security questionnaires submitted by suppliers, which can be reviewed if security-related questions arise.

To date, at least one supplier has been rejected by Lenovo because they would not provide sufficient information on the security questionnaire to allow the PSO to conduct a risk analysis. The ODTs have therefore been prohibited from using this supplier. As of the date of this letter, Lenovo has included 168 suppliers on the TSL.

**Windows 10 Pre-Load**

The following Lenovo product lines come with a pre-loaded version of the Microsoft Windows operating system: Lenovo Notebook, Desktop, ThinkPad, ThinkCentre and ThinkStation. In addition to Windows itself, PC vendors such as Lenovo typically also pre-load a variety of software applications that are intended to assist the customer with certain function (e.g., customer support) as well as to earn Lenovo additional revenue by charging the software vendors for inclusion in the pre-load.

The newest version of Windows—Windows 10—was scheduled to be released in approximately July 2015. With its release, Lenovo would again include a variety of additional third party and Lenovo-proprietary software as part of the pre-load package for new Windows 10 products ("Windows 10 Pre-Load").

In connection with its "Cleaner, Safer" initiative, in February 2015, Lenovo determined to implement a security review for every software application that was part of the Windows 10 Pre-Load. The decision to conduct this security review was made by senior officers within Lenovo and approved by Lenovo's Executive Committee. The CPSO was charged with creating and implementing the security process for the Windows 10 pre-load. Ultimate authority for the Win10 Process resides with the CPSO. The PSO supports the process.

The CPSO directed the establishment of a Software Security Review Board ("SSRB") to implement the security reviews and to make security-related determinations. The SSRB consists of a manager and representatives from the PSO and the relevant business units ("BU"). During the initial stages of the Win10 Process, the representatives of the PSO managed most of the security review process, but increasingly the PSO is training BU personnel to conduct initial security testing, with the PSO serving as advisors and resources.

The Win10 Process began with an inventorying of all software within Lenovo that were candidate applications to be included in the Windows 10 Pre-Load. The PSO and the SSRB directly contacted each Lenovo software development team within the relevant BUs (i.e., those producing Notebooks, Desktops, ThinkPads, ThinkCentres and ThinkStations) for an inventory of all Lenovo-developed software applications. The PSO and the SSRB also contacted each software product manager for each product to identify third party applications that were candidates for inclusion in the Windows 10 Pre-Load.

Lenovo engaged with a prominent software security firm in the Washington D.C. area to develop a proprietary tool for reviewing based on the Lenovo process to expedite the binary analysis of software applications for security vulnerabilities. The criteria for vulnerabilities was set forth in a series of contracts and statements of work between Lenovo and this security firm. The tool produces a report of identified potential security issues for each application. The report ranks the security vulnerabilities on a low, medium or high scale.

The PSO and the SSRB obtained a binary version of each candidate application for the Windows 10 Pre-Load and conducted security assessments for each approved application. Applications that scored a "low" vulnerability based on the tool were either approved for Windows 10 Pre-Load after assessment by the SSRB and the PSO (with final approval by CPSO) or were subject to security remediation. Among the "low" vulnerability applications that received approval without remediation were certain applications that are widely used in

industry and are produced by companies that are viewed as trusted, such that the overall risk associated by the application were acceptable to the CPSO. Those applications that scored as a "low" vulnerability but were designated for remediation, as well as any application that scored a "medium" or "high" vulnerability, were sent to one of Lenovo's two software security firms for further security review or were subjected to internal Lenovo security remediation. The security firms sent Lenovo a report for each such review on an application-by-application basis and detailed further findings regarding vulnerabilities.

After each remediation, all applications were subjected to retesting to ensure the vulnerability had been addressed. If a vulnerability could not be remediated, the SSRB (with the assent of the PSO) excluded the application from the Windows 10 Pre-Load unless the CPSO agreed that the overall risk associated with the application was acceptable.

Since implementing the Win10 Process, Lenovo has implemented a policy of not shipping any Notebook, Desktop, ThinkPad, ThinkCentre or ThinkStation with any Pre-Load software unless the software has been vetted through the Win10 Process and has been assessed to pass Lenovo's security parameters. That policy has been effectively implemented with the exception of a very small set of applications that inadvertently slipped through the process and were shipped without security reviews. Once these omissions were identified, the applications were immediately run through the Win10 Process, where it was confirmed that there were no unmitigated security risks associated with these applications. The Win10 Process has not been extended to include all firmware loaded on such products.

For the fiscal year ending March 31, 2016, Lenovo subjected 436 applications to the Win10 Process. Of those, 283 were approved and included in the Windows 10 Pre-Load, with 153 being rejected and/or still undergoing further remediation and testing. The Windows 10 Pre-Load process is ongoing.

Within Lenovo ThinkPad pre-load teams, any software application that is going to be pre-loaded on a product must be sent in binary form from the Lenovo product teams to a pre-load team that is managed by a pre-load manager. The pre-load manager is responsible for assembling all pre-load applications plus the operating system itself (Windows 10) in a "golden" software image that is ready to be loaded onto a product's hard drive during the manufacturing process. The golden image is stored on a "golden server" that is managed by the pre-load manager and his/her team. Lenovo's manufacturing facilities and contract manufactures pull the golden image from the golden server. The pre-load manager has ultimate authority and administrative rights to manage who can have access to the pre-load server. The pre-load team, under the direction of the pre-load manager, keeps an inventory of every application in any golden image. Golden images are retained in an archive on the golden servers. The pre-load manager also maintains a log of the source (by name) of each software application submitted for inclusion in a golden image.

During the Win10 Process, the SSRB and PSO kept an inventory of the file names, versions, and hash numbers associated with each application that had been reviewed and approved for inclusion in the Windows 10 Pre-Load. This inventory was given to the pre-load managers for use in assembling the golden images for each Windows 10 product. The pre-load teams manually inspected and compared the file names, versions and hash numbers of each application submitted by product teams (for inclusion in the golden image) against the listed provided by the SSRB and the PSO.

The pre-load managers represented to Chain Security that they had certainty that only approved software applications were included in the golden image for Windows 10 Pre-Loaded products, other than (as mentioned above) the small set of applications that inadvertently slipped through the process. Pre-load managers have identified applications submitted for inclusion in the golden image that were not approved in the Win10 Process and rejected those submissions. The pre-load teams digitally signed each golden image with their own unique digital signature after confirming that only approved software applications were included.

The CPSO and the PSO intend to further streamline the Win10 Process for future software security reviews, including placing more responsibility on the BUs to conduct and support the security testing. The PSO will remain a resource.

The initial SSRB is based in North Carolina, but Lenovo has just created a second SSRB in China that will focus on specific products for the Chinese market, with Chinese security standards to govern the security review. The Chinese SSRB will likely mirror the initial SSRB. The Chinese SSRB is using the resources of the PSO and is still subject to final authority of the CPSO, who has global security responsibilities for Lenovo products.

## CONCLUSIONS

Chain Security believes that Lenovo's implementation of the four identified components of the Program—Corporate Governance, Security Processes, Trusted Supplier Program and Windows 10—meet or exceed industry standards from a supply chain and product development security perspective and likely are at or above the level of its peers, including companies that are headquartered in the United States and currently provide products to the U.S. Government. In addition, Lenovo appears anxious and motivated to continue to improve its processes, and Chain Security is assisting them to do so, including with the implementation of BIOS Security and Software Lifecycle processes.

We are available to discuss the contents of this letter with you and/or other appropriate third parties. Please do not hesitate to contact me at 571.344.9625

(mobile)/csimkins@chainsec.com or Jeff Stern at 408.608.8184 (mobile)/jstern@chainsec.com. Our office number is 571.354.0068.

Sincerely,

Christopher P. Simkins

Chain Security, LLC
11490 Commerce Park Drive, Suite 200
Reston, VA 20191
571.306.2929 (direct)
csimkins@chainsec.com

# ATTACHMENT A

Qualifications of Chain Security, LLC

## Capabilities Summary

Chain Security

**Overview**

Chain Security is based in the Washington, DC area, with strong ties to Silicon Valley. Our team has deep technical and operational experience in government and commercial sectors. Our senior team members have built successful technology start-up companies and worked in government agencies, telecommunication carriers and defense contracting companies. Our technical experts and engineering team have hands-on experience designing, building and operating government and commercial programs and systems. We understand the full lifecycle of technology development, from design to sourcing to manufacture to deployment and customer support. Our experience allows us to assess the role particular technologies play in U.S. Government systems and operations and to understand how U.S. Government and critical infrastructure entities may view interactions of businesses operating in the U.S. with foreign owners, managers, investors, employees, vendors and subcontractors.

Chain Security also provides supply chain intelligence and analytics through its *Chain Security Intelligence* services. Through our analysis of supply chains and product development organizations, *Chain Security Intelligence* produces data-intensive supply chain models (using commercial visualization tools) that can show the commercial "chain of custody" for intelligent components (software and hardware) for specific technologies, from R&D all the way to deployed systems.

**Leadership**

*Christopher P. Simkins, Co-Founder and CEO*:
csimkins@chainsec.com; 571.344.9625 (mobile); 571.306.2929 (direct office)

Former Senior Official in U.S. Dept. of Justice (DOJ); investigator/prosecutor in DOJ's Counterespionage Section; reviewed over 200 transactions as DOJ's representative to CFIUS; CFIUS negotiator in a number of prominent transactions review where national security mitigation agreements were implemented; former senior corporate lawyer and current entrepreneur and consultant; breadth of experience helping U.S. and foreign companies do business and interact with USG interests and comply with U.S. regulations (e.g., CFIUS, export control, NISPOM)

*Jeffrey Stern, Co-Founder and COO*:
jstern@chainsec.com; 408.608.8184 (mobile)

Former Senior Vice President – Government Solutions, TerreStar Networks; technology executive with broad engineering, sales & marketing experience in mobile network design and emergency communications; executive leadership experience in both Silicon Valley and Washington, DC settings; multiple successful exits for start-up technology companies; co-founder Independence Technologies (BEA/Oracle); co-founder GoBeam, a Business VoIP SaaS pioneer (Covad Communications); consultant to multiple companies providing technical and operational solutions to U.S. Government customers

**ATTACHMENT B**

Lenovo Corporate Policy # 21 – Lenovo Product Security Policy (February 2, 2016)

***Confidential Information***

**Corporate Policy # 21 – Lenovo Product Security Policy**
February 2, 2016

Lenovo is committed to offering products that meet or exceed industry standards for security. Our customers must be able to use Lenovo's products with confidence that they have the tools that enable them to protect their data, and that our products minimize the risk of vulnerability to malicious or unauthorized use or attack by any third party. We deliver on these commitments by doing the following:

1. Including security as a design feature in all our products,
2. Adopting robust security practices
3. Appropriately managing and implementing security practices and processes throughout the entire lifecycle of our products.

We expect our employees and stakeholders, as well as our partners and suppliers, to support these commitments.

In furtherance of these security commitments, Lenovo is taking the following steps:

- Lenovo is implementing a broad product security program ("Product Security Program") managed by our Product Security Office, which reports directly to the Chief Product Security Officer ("CPSO"). This program encompasses critical security processes and practices implemented across product lines. All Lenovo employees and stakeholders are expected to comply with the Product Security Program, and to be responsive to the Program requirements. Lenovo will expect Partners and suppliers to make commitments in support of the Security Program as a condition of doing business with us.

- Lenovo appointed the Chief Product Security Officer as part of the agreement to purchase the System x Server business. The CPSO's original mandate was to oversee implementation of all security related activity regarding System x. This authority has been expanded to include all product lines within Lenovo.

- The CPSO is the Lenovo official designated with developing, implementing, and enforcing the Product Security Program, and will make final security-related decisions for all Lenovo products. Lenovo will ensure that the Product Security Office has all necessary corporate authority and resources to carry out these responsibilities.

It is clear that the security of our products is a key factor in our customers choosing Lenovo as their supplier of IT equipment.

Yuanqing Yang, Chief Executive Officer

# ATTACHMENT C

## Lenovo Corporate Policy # 21 (revised) – Lenovo Product Security Policy (August 3, 2016)

**Corporate Policy # 21 – Lenovo Product Security Policy**
August 3, 2016

Lenovo is committed to offering products that meet or exceed industry standards for security. Our customers must be able to use Lenovo's products with confidence that they have the tools that enable them to protect their data, and that our products minimize the risk of vulnerability to malicious or unauthorized use or attack by any third party. We deliver on these commitments by doing the following:

1. Including security as a design feature in all our products,
2. Adopting robust security practices
3. Appropriately managing, implementing, and validating security practices and processes throughout the entire lifecycle of our products.

We require our employees and stakeholders, as well as our suppliers, to support these commitments.

In furtherance of these security commitments, Lenovo has taken the following steps:

- Established a comprehensive product security program ("Product Security Program") managed by the Corporate Product Security Office (PSO), which reports directly to the Chief Product Security Officer (CPSO). This program encompasses critical security processes and practices being implemented across product lines. Lenovo employees and stakeholders are required to comply with the Product Security Program, and to be responsive to the Program requirements. In addition, Lenovo requires suppliers to make commitments in support of the Security Program as a condition of doing business with us.

- Identified the corporate Chief Product Security Officer (CPSO), and designated the CPSO as the Lenovo official responsible for developing, implementing, and enforcing Product Security Programs and processes across Lenovo. The Product Security Office under the CPSO has the authority and resources to carry out these responsibilities.

- Authorized the PSO to develop and implement industry leading security best practices

In addition to the above items, Business Units may incorporate additional controls to meet specific regulatory or customer requirements.

It is clear that the security of our products is a key factor in our customers choosing Lenovo as their supplier of IT equipment.

Yuanqing Yang
Chairman & CEO
Lenovo

# ATTACHMENT D

## Program Policy Issued by Chief Product Security Officer

### IMPLEMENTATION OF LENOVO'S PRODUCT SECURITY PROGRAM

Cyber security is a critical requirement for individuals, corporations, and institutions in today's economy. Our customers demand products and strategies that protect their computers, networks, programs, and data from unintended or unauthorized access, change, or destruction. To address the ever-changing demands in this area, Lenovo is implementing a broad product security program ("Product Security Program") that is being managed by Lenovo's Chief Product Security Officer ("CPSO") and the Corporate Product Security Office ("PSO"), which reports directly to the CPSO. This program signals Lenovo's commitment to product security by building upon and strengthening existing policies and processes, and centralizing management and attention to these issues. The program was highlighted by Lenovo's Chief Executive Officer in a Corporate policy statement dated February 2, 2016, as an essential part of our commitment to customers, and as a key to our future success.

This Product Security Program encompasses critical security processes and practices to be implemented across our product lines. All Lenovo employees and stakeholders are required to comply with the Product Security Program, and to be responsive to the Program requirements. Security principles, policies, and best practices are reinforced through compliance training for all Lenovo employees, and through more detailed courses based on an employee's specific job requirements. Suppliers will also be required to make commitments in support of the Security Program as a condition of doing business with Lenovo.

The CPSO (with the support of the Product Security Office) has authority and responsibility for ensuring full implementation of the Product Security Program. The PSO serves as Lenovo's Center of Excellence for product security, supporting product security matters across all product and customer segments. Lenovo employees with product security concerns, including those from customer inquiries, should directly contact the Product Security Office (psirt@lenovo.com).

The Product Security Program consists of initiatives that address product security throughout the product lifecycle. Program documentation is posted on Lenovo's internal website (*see* http://lenovocentral.lenovo.com/product-security/ . Lenovo's commitment to the Product Security Program is also outlined on Lenovo's external website (*see* http://www.lenovo.com/us/en/product-security/landing.shtml).

Product Security program documents posted in Lenovo Central will focus in the following areas:

- Overall Product Security Governance, including:
  - Corporate Product Security Policy
  - Product Security Program Document
- Software Programs, including documents relating to:
  - Strategic SW Process: Lenovo Secure Development Lifecycle, or LSDL (Standards and Processes)
  - Windows 10 Tactical Review Standard (SSRB Process)
  - BIOS Manifest Process
- ODT Governance Process, with documents relating to:
  - Integration of governance into the Platform Integrated Offering Delivery (IOD) process
  - Security responsibilities of all ODT members
- Supply Chain, including:
  - The Trusted Supplier Program
  - The Trusted Supplier List
  - Parts shipment, Manufacturing, and Finished Goods Shipping
- Product Security Incident Response, including:

**(ATTACHMENT D cont.)**

  - Product Incident Response Team (PSIRT)
  - Incident Response Process Flow
  - Advisories

- Product Security Training

In addition, under the Product Security home page on Lenovo Central, there are several policy documents, as well as some past presentations that have been used to inform customers of Lenovo's Security actions.

As mentioned, all employees are required to follow these initiatives. Each employee should be working with their manager to develop an individual security training plan, based on their job requirements and the provided curriculum.

If you have any questions or comments, please contact the Product Security Office.

Daryl Cromer, Lenovo Chief Product Security Officer