UNITED STATES DISTRICT COURT

DISTRICT OF NEW MEXICO

STC.UNM, Plaintiff, v. INTEL CORPORATION, Defendant.	Civil No. 1:10-cv-01077-RB-WDS

DECLARATION OF MALCOM HARKINS IN SUPPORT OF INTEL'S OPPOSITION TO STC'S MOTION TO COMPEL AND IN SUPPORT OF INTEL'S MOTION TO AMEND THE INTERIM PROTECTIVE ORDER

1. My name is Malcolm Harkins. I have personal knowledge of the facts stated below and would testify that they are true if asked to do so. I am making this declaration (1) to oppose STC's efforts to discover commercially valuable and carefully guarded trade secret information about research and development into future manufacturing technology that will not be complete or used to make commercial products until after the patent that STC is asserting against Intel has expired, and (2) to support Intel's motion for a protective order.

2. I am Chief Information Security Officer and General Manager of Intel's Information Risk and Security Group, which is responsible for all aspects of information risk and security controls and compliance at Intel. These responsibilities include establishing and maintaining corporate-wide information security policies, standards, and procedures designed to protect Intel's confidential information, driving compliance to regulatory requirements that affect Intel information (such as export/import controls), training all employees so they can adhere to Intel's information protection policies and procedures, and overseeing the overall protection of information. In addition, Intel regularly audits its procedures to ensure compliance.

3. My duties include securing confidential information, including information about Intel's manufacturing processes. The protections and safeguards described in this declaration are in addition to the extensive efforts designed to secure Intel buildings and confidential Intel documents.

4. Intel's information security procedures cover all aspects of how Intel employees are required to protect Intel's financial, technical, marketing, and sales information. For example, these procedures mandate how Intel employees must classify documents that are sensitive, how Intel employees must handle such classified documents and other media, how Intel employees must securely store classified information in electronic format, the requirements to encrypt digital media, and how to transport media containing classified information.

5. Intel has three levels of security for Intel information: confidential, restricted secret, and top secret. The highest level of security is "top secret," and it is reserved for our most sensitive and valuable information. Intel's process technology data and documentation ("process information") is classified at this highest "top secret" security level because Intel regards that information as some of its most important assets.

6. Intel takes great efforts to secure any hard copies made of its process information. Intel has two levels of security for hard copies of especially sensitive documents—orange (for restricted secret information) and red (for top secret information). Any hard copies of process information would be top secret red documents. Anyone who seeks a hard copy of any portion of top secret information must have a need for it, and his or her need to know must be approved by the project manager or general manager of the area that owns the information. Intel employees must follow extensive procedures that are enacted and enforced by my department. Failure to follow these procedures is the basis for discipline, up to and including termination.

7. Hard copies of top secret documents are given serial numbers for tracking purposes and bound in a red cover that sets forth the top secret classification of the document, who is authorized to see the document, and instructions on what to do if the document is found. This serialized document is assigned to the specific employee authorized to have it. It may not be copied or distributed. Indeed, the employee must keep the document in his or her physical possession or have it under lock and key in an Intel-provided special locking cabinet. The document may never be left unattended without being properly secured. The document then must be returned to one of Intel's worldwide registered confidential document service centers. It may not be disposed of in any other way.

8. Protection of our electronic process information is extraordinary and goes beyond even the intense efforts to secure Intel buildings and to guard hard copies of the process information. Intel guards its electronic versions of process information even more closely than hard copies because of the ease with which electronic files may be copied and distributed.

9. Intel imposes even greater protections for electronic process information than its general network and computing security measures. For example, information about the process for coating a layer of photoresist before the lithography step is segregated to a database limiting access to only specific engineers of the group working on that particular aspect of the process flow. Even members of Intel's Technology and Manufacturing Group ("TMG"), such as engineers working on other aspects of the process technology, are not permitted access to the database without the approval of the General Manager of TMG. Anyone outside TMG also must get direct permission from the General Manager of TMG to access the information. Intel controls this separate access by requiring additional authentication, such as second-level passwords and/or maintaining a list of approved user identifications that is used to control

access. That list of approved user identifications is updated whenever there are changes such as employment termination. Additionally, the list is updated at least every 24 hours to ensure that only those employees with proper need to access the data are allowed on the network. Indeed, that list may be updated within minutes if there is a need for immediate update. Intel has implemented an auditing and monitoring program to ensure compliance with these restrictions.

10. Engineers working on process technology must access the computer and file servers on the network where the process information is stored. Any piece of process information that is considered in a state of rest for storage on a file server (e.g., share drives, P drives), application server (e.g., SAP, DB, voice or e-mail), intranet servers, or manufacturing or engineering server must have an additional level of protection (encryption, for example). Process information may never be placed on any extranet or internet servers or internal social computing platforms.

11. When Intel installs its process information on a stand-alone computer at its outside counsel's office for this case, a trusted individual, such as an employee or contractor approved by Intel, will have to fly to that location with the electronic materials physically with him or her at all times in order to deliver it to the secure location. When I say that the electronic materials must be physically with that individual at all times, this means that it cannot be placed into checked baggage, and in fact cannot be left unattended even for a short period of time.

12. There is significant danger of disclosure of process information if it is not maintained by Intel on a stand-alone computer in a secure location. Similarly, there are risks associated with non-Intel employees storing print-outs of process information at several locations with varying degrees of security. There is a very real risk that, if treated in this manner, the process information could be stolen, intercepted, misdirected, or lost and utilized by someone

seeking to profit from some of Intel's most valuable assets. Intel guards against those efforts by ferociously guarding its process information. Intel spends upwards of $60 million each year to secure and safeguard its confidential and secret information. That effort involves 300-400 people worldwide.

13. All of Intel's intense efforts to guard its process information would be put at risk if that information were kept in the home of a person who is not even an Intel employee. Handing over our process information to someone whose job is not to protect Intel's interests or comply with its security procedures means that Intel relinquishes control over some of its most precious assets.

I declare under penalty of perjury that the foregoing statements are true and correct.

Dated: 4/5/11 at Folsom, CA.

Malcolm Harkins

Certificate of Service

The undersigned hereby certifies that on April 5, 2011, the foregoing document was electronically filed with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to all counsel who have entered an appearance in this action.

ATKINSON, THAL & BAKER, P.C.

/s/ *Clifford K. Atkinson*
Clifford K. Atkinson

20336-1313/LEGAL20511359.1