THE ISA GUIDELINES FOR SECURING THE ELECTRONICS SUPPLY CHAIN

By Scott Borg

Contents

General Principles

The purpose of these guidelines

- These guidelines are instructions for securing the global electronics supply chain. They describe the security procedures that need to be implemented at each of the various stages in the production of electronics products. This systematic effort to secure the electronics supply chain has become necessary, because electronics manufacturing is now a series of intricately connected processes that need to be distributed across many different countries and regions in order to maximize quality while minimizing cost.

- The primary purpose of these guidelines is to protect global electronics companies from major economic losses.

  The sorts of losses that need to be prevented include:
  I) losses due to interruptions or delays in production, including those due to false or misleading reports on production start dates, available capacity, production rates, quality test results, inventories, and delivery dates;
  II) losses due to diversions or corruptions of production, including the outright theft of parts and products, insider sabotage, the counterfeiting of electronic products, and the substitution of inferior components;
  III) losses due to the discrediting of processes or products, including uncertainties about quality, concern about product support, and adverse publicity involving the treatment of workers, environmental impact, and business affiliations;
  IV) losses due to the theft of competitively important information, including diffuse, but competitively important business and production information, as well as recognized intellectual properties.

  The enormous scale of the losses that global electronics companies have suffered due to these security problems in their supply chains means that there is now an enormous incentive to implement guidelines of this kind.

  These guidelines are *not* intended to burden electronics manufacturers with more costs. The security measures included in them are intended to pay for themselves many times over by reducing losses. Collectively, these security measures should ultimately deliver considerable increased profits by allowing the implementation of more efficient and advanced global manufacturing.

- In addition to benefiting global electronics companies, these guidelines are designed to help existing electronics suppliers claim credit for their security achievements and to better protect their own interests. Explicitly identifying the security procedures that electronics suppliers are expected to follow should provide a competitive advantage to the companies that are doing a good job of implementing these procedures. Meanwhile, these security guidelines should help electronic suppliers protect themselves from physical thefts, damage to reputation, loss of intellectual property, and many of the other types of damages that global electronics companies also need to avoid.

- These guidelines should help, not just existing electronics companies, but also companies and countries that wish to become electronics suppliers. This is because the guidelines spell out exactly what will be required of new entrants to the electronics markets as far as security is concerned. Once companies and countries know these requirements, it becomes much easier for them to satisfy the security concerns of their potential corporate customers. In addition to providing those companies and countries with new opportunities for economic development, the result should ultimately be a more geographically diverse and, hence, more resilient electronics supply chain.

- These guidelines should therefore be used as a reference document in the drafting of contracts between the producers of electronics products and their suppliers. They should be applied in a way that coordinates security throughout the electronics supply chain and that provides a common standard that competing bidders should be expected to meet. Establishing a common set of expectations about what security measures will be specified in electronics supply contracts should also greatly reduce the time and costs of negotiating those contracts.
- Governments will have ample reason to support the adoption of these guidelines. This is because implementing these guidelines will make it enormously more difficult to insert malicious firmware or defective or malicious components into electronic products destined for use by military forces or critical infrastructure industries. Since most direct programs to secure electronics manufacturing for government and military use have little hope of being economically viable, the best hope governments have of securing their electronic systems is to make this effect a by-product of a security program instituted entirely for other business reasons.
- These guidelines should help the electronics industry to secure even more of the benefits of sensible globalization. If electronics manufacturing utilizes sufficiently effective security measures, and if there is sufficient reason to believe that these security measures are being carried out in good faith, then it ideally shouldn't matter who carries out any manufacturing phase, where that manufacturing phase is being carried out, or who owns the facility that is being used for it.
- The overall result of these guidelines should be a more efficient, fairer, and more resilient electronics supply chain, with lower risks for every participant.

The general principles for applying these guidelines

- The point of these guidelines is to deliver technical and economic results, not put companies through more administrative formalities. Hence, these guidelines describe the actual, operational procedures that need to be carried out, not the administrative arrangements or policy declarations that might be necessary to implement these operational procedures.
- These guidelines are shaped as much by economic considerations as by technological considerations. Every security measure needs to have a cost that is significantly less than the probable loss of value that the security measure is preventing. In other words, every security measure needs to be cost-effective. If any "best practice" is really the best practice from a business or economic standpoint, it should be made a standard practice.
- Many of these guidelines do not describe security measures as such, but instead describe ways of carrying out manufacturing operations. This is because the most cost-effective way to deal with many security issues is not to add extra protective measures, but to arrange the way business is done so that extra protective measures become unnecessary or, at least, much cheaper.
- It should always be made legally and contractually possible to dispense with any given security measure if a more effective measure is substituted instead, but the producer of the final product will need to acknowledge that the security measure being substituted is indeed more effective.

- The corporate customer that is responsible for the final product may wish to excuse some suppliers from carrying out some of these security measures if those security measures are not important for a particular and if dropping those security measures would significantly reduce the suppliers' costs. A consumer product that has no chance of being used in a critical application, for example, does not need to be as carefully protected from the insertion of counterfeit parts and malicious firmware. Similarly, a product that is truly generic and contains no distinctive intellectual property does not need to have its design features protected from intellectual property theft.

  However, care should be taken in relaxing the security in facilities that will need to be secure for the production of other products. Many of these security measures, once instituted, cost very little to keep in place. Relaxing these security measures part of the time and then tightening them the rest of the time may actually increase costs. Once security measures have been temporarily relaxed, it may become much more difficult to persuade employees to maintain them in the future. Altogether, attempting to save money by selectively or temporarily relaxing these security measures may turn out to be a poor economy for all concerned.
- The security measures marked here with an asterisk***** are greatly needed and potentially cost-effective, but currently difficult to carry out, because the necessary tools and services are not yet readily commercially available. Hence, while serious consideration should be given to instituting these security measures, doing so may not yet be cost-effective for many manufacturers.
- An effort has been made throughout this document to adjust the language so that the guidelines will be comprehensible to those who are not technical specialists, who come from different parts of the industry, or who have different linguistic backgrounds. It is hoped that the resulting use of fresh language to describe many security procedures will also cause security professionals to stop and think about what is really involved in each security measure.

The supply chain phases used to organize these guidelines

- The successive phases, into which these guidelines are organized, represent the stages nearly every electronic product goes through. They start with the products conception and then run through (1) the design process, (2) the production of the photomasks to be used in the manufacture of the microelectronic components, (3) the actual manufacture of those microelectronic components, (4) the manufacture of the printed circuit boards used to connect and hold the other electronic components, (5) the "pre-assembly" of those components into loaded circuit boards, (6) the assembly of the actual electronic products, (7) their distribution though intermediary steps to end-users, and (8) the maintenance they receive during their usage life, ending with their disposal.
- All these phases of the electronic supply chain are remarkably the same whether the electronic product is a laptop computer, a server, an airplane, a smart phone, a router, a gaming console, or a credit card reader.
- In addition to covering each stage in the manufacturing process, these guidelines include a section (9) on the legal conditions that need to be in place for the rest of the guidelines to be implemented effectively. Some of these legal conditions can be put in place by the corporations involved, but others need the legislative and governmental support of the countries endeavoring to gain or maintain a competitive position in the global markets for electronics manufacturing.

- The guidelines for each phase of the electronics supply chain are designed to be complete and self-contained. Hence, only one section of the guidelines will need to be applied to any given phase of production. Accomplishing this required a modest amount of repetition, but there was no good way to avoid this, because hardly any of the repeated guidelines were repeated throughout every phase of production.
- The complete guidelines outlined in this document may seem lengthy, but the guidelines for securing any single phase of the electronics production process are not. The complete set of guidelines needed to be conceived and developed together, because the security measures instituted in one phase of the electronics supply can have a profound effect on the security measures that are needed in other phases. When it comes to implementing these guidelines, however, they can generally be treated as nine separate sets of guidelines. This means that the number of guidelines that will need to be incorporated into any given supply contract is actually not very large.

The process by which the guidelines were produced

- These guidelines are all based on recommendations and anecdotes from people with extensive field experience. Nearly every guideline included here is currently the normal practice of some global electronics company in some portion of its operations. Most of these practices were instituted in response to actual security problems that have resulted in considerable losses or could have resulted in considerable losses. Although the people responsible for these security practices were able to describe them in detail, many of these practices do not seem to have been previously codified or made into written policy.
- The original basis for these guidelines was an extensive series of conferences, workshops, and meetings organized and sponsored by the Internet Security Alliance over a period of roughly four years. The participants in these events included representatives from forty-six corporations, six government departments or agencies, five research institutions, a law firm, and two trade associations. The individuals involved are listed at the end of this document, except for a small number who wished to remain anonymous. The main results of these conferences, workshops, and meetings were long lists of security problems, numerous anecdotes about particular security cases, and a large collection of comments about relative security priorities and points that deserve special attention.
- Based on these discussions, Scott Borg carried out large numbers of interviews with individual experts who had dealt in field situations with the specific security issues that had been identified. These experts provided step-by-step descriptions of the individual operations that needed to be secured, the security measures that needed to be taken to secure those operations, and other measures that had been tried, but abandoned as ineffective or too expensive for what they accomplished. The individuals and companies involved were extraordinarily generous in sharing their best practices. It is these actual practices that provided the material for these guidelines.
- The drafts of individual guidelines were all based these interviews with individual experts, along with periodic reviews of the conference and workshop records. In many cases, there were multiple interviews addressing the same point, which then had to be collated, studied, and evaluated. The drafting of each individual guideline was thus the outcome of a fairly elaborate process, even before the various drafts were sent back to the contributing experts for review.
- All of the actual guidelines were drafted by Scott Borg, except for about twenty legal guidelines that were drafted by Nick Akerman. No guidelines were drafted by anyone else. The drafts of the guidelines were circulated extensively for comments among the workshop

participants and among the specialists in each facet of electronics supply chain security. As the comments were collected, the drafts were repeatedly revised and re-circulated until virtually all of the best qualified security experts for each phase of the electronics manufacturing process were satisfied with them.

The efforts to make sure these guidelines are cost-effective

- Every guideline that was considered for inclusion in this document was examined carefully from the standpoint of cost-effectiveness. This resulted in many familiar security measures being deliberately omitted, at least for certain phases of the supply chain. It also resulted in some relatively unfamiliar security measures being included. Some of the security procedures that had previously been standard practice were intentionally dropped, because no rationale for their continued use was provided. Meanwhile, other security measures that might sound odd or "excessively fussy" have been included because they were found in practice to be efficient ways of dealing with important real-life security problems.

- The stringency of the security measures and the degree of detail in the guidelines has been carefully adjusted to fit the probable level of risk in each operation and at each stage of the supply chain. Thus, for example, the security guidelines for the design phase are much more elaborate than the security guidelines for the circuit board pre-assembly phase. This is because the harm that could be caused by insufficient security in the design phase is much greater than the harm that could be caused by insufficient security in the circuit board pre-assembly phase.

- The emphasis here is not on doing as many things as possible to secure each phase of the manufacturing supply chain, but on doing the right things. Some readers of these guidelines will probably find that the security measures that have been included suggest additional measures that have been left out. In most cases, these omissions are deliberate. The additional security measures, which seem like obvious steps to take, were reveled on closer examination to be ineffective or superfluous, given the other measures and systems in place. The few exceptions, where measures of limited effectivenes were retained in these guidelines, are generally cases where the measures in question serve legal purposes, laying the ground for possible legal actions.

- A special effort was made to avoid mechanically repeating the same security measures in different production phases. Often when people drafting standards and guidelines have identified a useful security measure, they assume that it should be applied everywhere. But the same security measures have very different costs and yield very different benefits in different phases of the supply chain. Repeating a security measure that is vital at an early stage in the supply chain may be a complete waste of resources at a later stage in the supply chain.

- Some guidelines are included here that would not have been cost-effective as recently as two or three years ago, but have now become cost-effective, due to the falling costs of data storage and electronic equipment. It is now practical, for example, to record and store large quantities of access logs and high-quality surveillance videos that would have been too expensive to keep only a few years ago.

- Most of the security measures that have been included in these guidelines are remarkably inexpensive if they are built into the architecture and operating procedures of the various production phases when the operations and facilities are being laid out or when they are being structurally renovated. These security measures will only seem burdensome if, instead of being integrated into the operational planning, they are tacked on later as a kind of afterthought.

- Because many of these security measures need to be built into the architecture and operating procedures of the various production facilities, it is recommended that the companies that will be expected to carry out the security measures be allowed a reasonable period of time to phase them in. However, it would be reasonable to give preference in the awarding of supply contracts to those companies that are already carrying out these security procedures or that will be able institute them sooner.
- Because several of the factors that determine the cost-effectiveness of security measures are changing over time, the cost-effectiveness on each security measure will need to be regularly re-evaluated.

The need to understand the guidelines' collective functions

- Many of the individual guidelines have a beneficial effect on security only when used in conjunction with other guidelines. Hence, care should be taken in relaxing any one of these guidelines or substituting a different security measure, because several other guidelines may be affected.
- Many of the individual guidelines are accomplishing several things at the same time. Hence, if one effect of the guideline becomes less important, other effects may remain as important as ever.
- There is no substitute for a sincere and thoughtful effort to provide good security. This effort needs to be informed by a wider vision of the factors that collectively determine risk, including the changing nature of the threats, the possible consequences of various security lapses, and the new methods under development for reducing vulnerabilities.
- The wider vision that provides a context for the application of these guidelines and the theoretical concepts that underlie them are beyond the scope of this current document. They can be found in other literature, including "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework" (2009) and *Cyber Vulnerability Analysis* (forthcoming), in which the author of these guidelines discusses the theory and rationale behind them.
- To be genuinely effective, these guidelines will need to be applied, not mechanically, but in good faith and with understanding.

The relationship of these guidelines to other check lists, standards, and guidelines

- These guidelines were drafted entirely from scratch, without reference to any other check lists, standards, or guidelines. This is because there had previously been no comprehensive attempt to describe the practices necessary for securing electronics manufacturing. There have been check lists and guidelines aimed at securing many related things, including: corporate and government information systems, software products, software development processes, computer networks, and telecommunications systems. But the secure manufacturing of electronic equipment, on which most of these other things rely, has not been previously tackled in any thorough or systematic way. The fact that this was a pioneering effort made it easy to take a fresh look at the subject, but it also made the work progress slower than it might have been otherwise.
- These guidelines are not intended to replace guidelines and standards that describe general cyber security measures, but should be used in conjunction with those. The current guidelines describe how to limit the types and extent of the information systems deployed in electronics manufacturing facilities. They also describe some special cyber security measures that need to be implemented in the certain parts of the electronics manufacturing

process. But any information system employed by electronics manufacturers will still need to be secured in standard ways, and other, more general cyber-security guidelines will be helpful with that.

- These guidelines are also not intended to replace guidelines and standards that focus more narrowly on the cyber security of automated industrial control systems. Securing automated controls is an important part of a layered defense strategy for manufacturing facilities. Hence, the special security measures that can be taken to reduce the vulnerabilities of programmable logic controllers (PLC's), distributed control systems (DCS's), and other automated controls should be implemented wherever possible in electronics manufacturing facilities.

- The guidelines and standards that these current guidelines *are* intended to replace, at least where electronics manufacturing is concerned, are the guidelines that were not designed specifically for the electronics supply chain, but have been used for this type of supply chain in the past, because nothing more appropriate was available. These other types of guidelines include guidelines originally intended to provide security for general manufacturing, for other types of supply chains, and for software development. Guidelines of these kinds may be useful in securing operations that are complementary to electronics manufacturing, but they are not sufficient or even appropriate for securing the manufacturing of the electronics hardware itself.

- During the more than four years in which these guidelines have been under development, a number of other efforts concerned with the security of electronics manufacturing have gotten underway. The people involved in these other efforts were invited to the ISA workshops, and several of them became regular participants. The people involved in the other efforts were also provided with the reports, preliminary findings, and earlier guideline drafts that emerged from the ISA-sponsored effort. Meanwhile, a number of electronics manufacturers had begun to codify their security procedures. As they did this, they were encouraged to draw on the findings of the ISA workshops and to offer suggestions for the guideline drafts as these were being developed. As a result, there has been considerable informal coordination between these efforts, and the information and insights embodied in these guidelines have already been very influential.

- One of the useful complementary documents produced by participants in the ISA electronics supply chain workshops is *NISTIR (Draft) 7622: Piloting Supply Chain Risk Management Practices for Federal Information Systems* (2010), by Marianne Swanson, Nadya Bartol, and Rama Moorthy. This provides an overview of some relevant administrative and policy requirements, as well as highlighting some security measures that are of special importance.

- Because these guidelines focus on the concrete security measures that need to be implemented, rather than on the procedures and policies necessary for implementing them, organizations employing these guidelines may wish to supplement them with other guidelines or standards that focus on administrative procedures. One of the most useful and best known of these other standards and guidelines is the *ISO 27001*, which focuses on the management procedures for information security systems.

1. The Product Design Phase

General product design

Procedural policies to be followed throughout the design process

1.001 Initiate the planning and tracking of security provisions at the very beginning of the design process, so that they become part of the work procedures for each step.

1.002 Limit the personnel with access to the design facilities to those who genuinely need to be there.

1.003 Document the arrivals and departures of all personnel entering the design facilities.

1.004 Use two or three factor authentication (e.g., photo RFID and fingerprint) for all personnel entering and leaving the design facilities, unless the design team is small enough so that the relevant security staff and the members of the design team all know each other.

1.005 Make sure design meetings are held in rooms that do not adjoin public areas or have public-facing windows.

1.006 To the extent legally permissible, scan everyone entering or leaving the design facilities for devices that could be used to capture or transport large quantities of information, such as personal laptops, flash drives, iPods, digital cameras, CD burners, and CD's.

1.007 Do not allow mobile devices (e.g., cell phones, smart phones, tablets) to be brought into any important design meetings because they can be remotely accessed and turned into listening devices.

1.008 Make sure the networks used in the design process are completely isolated from the other corporate networks.

1.009 Require two-factor authentication for any access to the computers used in the design process.

1.010 Set the access controls in the design facility's information systems so that they only allow an employee to access the systems and documents deemed necessary for that employee's work assignment.

1.011 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

1.012 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

1.013 Maintain regular logs recording which personnel access which design documents or data and at what times.

1.014 Arrange for any abnormally large downloads of design information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

1.015 Record which parts of the design documents each person generates, writes, or revises.

1.016 Make sure any transmission of designs or data relevant to the designs is strongly encrypted if it is being sent to an outside partner or to a different physical facility.

1.017 Make sure the computers and other equipment used in the design process cannot be physically accessed by outside personnel, such as cleaning staffs.

1.018 If cleaning staff or other maintenance personnel need to be admitted into rooms where equipment containing sensitive design information is stored, these people should either be given the same sort of background check as the design personnel or else be personally escorted by a trusted member of the design team, as well as having their actions video taped.

1.019 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information employed in the design process and, depending what is uncovered, bring appropriate remedial, employment, and/or legal action.

Personnel policies to be followed throughout the design process

1.020 To the extent legally permissible, make sure all personnel who will be admitted to the design facilities are given a thorough background check, including financial identifiers and employment histories.

1.021 Require each contributor to the design process to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them.

1.022 Require each employee in the design process to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

1.023 Conduct entrance interviews in which each person joining the design team confirms his or her understanding that no trade secrets, confidential data, or other intellectual property from previous employers can be used on this design project.

1.024 Require each employee in the design process to sign an agreement specifying that he or she has not retained documents from a previous employer containing trade secrets, confidential data, or other intellectual property.

1.025 Explicitly define the limitations on the physical and digital access privileges of each employee.

1.026 Require each employee to acknowledge the limitations on his or her physical and digital access privileges.

1.027 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

1.028 Impress upon the design team the need to refrain from discussing design problems and goals in places where people outside the design team are present, such as company cafeterias and elevators.

1.029 Make sure design personnel are not given work assignments that would inevitably lead them to draw on trade secrets, confidential data, or other intellectual property from their previous employers.

1.030 Make sure that an employee's physical and digital access to the design facilities and their information systems is ended at the same time his or her work responsibilities inside those facilities are ended.

1.031 Conduct exit interviews in which anyone leaving a company involved in the design process confirms his or her understanding that *no* knowledge of trade secrets, confidential data, or other intellectual property acquired or created during work for that company can be used in future jobs.

1.032 Warn design personnel who are leaving the company that any physical or electronic information pertaining to the design process must be securely destroyed or returned to the company, including rough notes and drawings used to jot down design ideas.

Specification of the overall physical design features and the electronic inputs and outputs

1.033 Make the designers aware that they are responsible for designing the product in such a way that it can be produced securely.

1.034 Make the designers aware that they are responsible for designing the product in such a way that the company's intellectual property cannot be easily extracted from the finished product.

1.035 Make the designers aware that they are responsible for designing the product in such a way that the product does not cause security problems for the end-users.

1.036 Make the overall physical requirements for the product restrictive enough to minimize the space available for illicit add-ons, such as wireless receivers and transmitters.

1.037 Make the product specifications *complete enough* so that covert modifications or additions would be more difficult.

1.038 Make the product specifications *narrow enough* so that covert modifications or additions would be more difficult.

1.039 Require the design staff to be trained (and given an annual refresher course) in the current techniques for hacking hardware and the ways product design needs to take account of security.

Modularization of product design

Breaking the design into modules and determining their production methods

1.040 When dividing the design into functional modules, consider where customized modules, rather than generic ones, could add robustness, as well as where they could add capabilities.

1.041 If possible, include security features in the specifications of the modular inputs and outputs.

1.042 Where possible, design "loose-couplings" between critical modules, so that privilege limitations can be introduced between modules, and so that a compromise of one module doesn't always compromise all the rest.*

1.043 Make the protection of intellectual property, as well as direct cost, a major factor in deciding which modules should be components manufactured directly, which should be components that are outsourced, and which should be components that are purchased.

1.044 Specify the electronic inputs and outputs of critical, custom-made components with enough precision to limit the latitude for deviations from the specified design.

1.045 Investigate the security, as well as the performance, of any pre-existing modular designs that are going to be purchased from outside developers.

Simulation of modular interactions

1.046 Explicitly determine the performance range that can be tolerated from each component, given the ways other components might be affected by it.

1.047 Explicitly determine the relative criticality of each component, considering the difficulty and cost of replacing it, the degree to which its performance can vary without seriously undermining the product’s main functions, and the extent to which its likely malfunctions could damage other components.

1.048 Explicitly determine the relative criticality of each “bus” that transfers data between components, identifying the ways in which the signals traveling through it might be improperly blocked, modified, tapped, or redirected, and assessing the consequences of those actions.

Schematic product design

Creation of schematic diagrams using circuit design software

1.049 Compartmentalize design operations to protect intellectual properties.

1.050 Turn off unneeded schematic development tool options.

1.051 Make sure each human operation in the application of the circuit design software is verified or reviewed by a second person.

1.052 Limit the privileges of those working on the circuit designs to their areas of responsibility, so that they cannot access other portions of the circuit designs.

1.053 Document each schematic design operation, including those that resulted in discarded options, noting who carried out which operation, and when they did it.

1.054 Make sure the hard disks used in the schematic design process are securely wiped and reloaded with the original design software before being used for different projects.

Testing of detailed circuit designs in simulations

1.055 Verify the validity and integrity of the simulation software.

1.056 Protect the simulation software from alteration after its validity and integrity has been verified.

1.057 Verify the validity and integrity of any patches or upgrades before these are applied to the simulation software.

1.058 Remove test features and any access passwords before passing the design on.

1.059 Use the circuit simulations, not just to verify that the circuits will function as planned, but also to verify or correct the previous assessments of each component’s and bus’s criticality.

Security features instituted in the circuit design to protect against tampering and theft of intellectual property during the later phases of the production process

1.060 Withhold information about each component’s intended use from the documentation that will be sent along with its design to those responsible for producing it.

1.061 Reserve key design components to the downloadable firmware of a chip, so that the physical chip is not functional until that firmware has been downloaded onto it.

1.062 Incorporate a design lock in the chip, so that the chip can’t be employed without the key to that design lock.

1.063 Create some secret performance tests with results which will not be available to the fabrication personnel or deducible by them, but which will provide a good indicator of whether the chip has been fabricated faithfully.*

1.064 Identify or create digital characteristics in the design that would be changed if the design were augmented with additional circuits.*

1.065 Recognize that having electronic components fit snuggly into their housings is an important security feature, since it hinders illicit add-ons.

Physical product design

Creation of physical circuit layouts using circuit layout software

1.066 Stringently separate the network containing the circuit layout software from other corporate networks.

1.067 Make each human operation in the application of the layout design software a two-person effort.

1.068 Check the circuit layout designs to make sure they have special features that were secretly predicted from the schematic diagrams.*

Computer-aided steps to produce physical layout of mask layers

1.069 Stringently separate the network containing the software for the physical layout of mask layers from other corporate networks.

1.070 Limit the personnel with physical and/or digital access to the network containing the software for the physical layout of mask layers.

1.071 Document the arrivals and departures of the personnel accessing the work stations connected to the network used for the physical layout of mask layers.

Transmission of wafer mask physical layouts to the wafer mask production facility

1.072 Convey the physical layouts for the wafer masks to the wafer mask production facility either (a) using a virtual private network (VPN) that allows direct instruction of the machines writing the masks, or (b) using a secure server that is being employed as a “drop box” to allow downloading of information over an encrypted connection.

1.073 If a secure server is being employed as a “drop box,” make sure the information placed in it is strongly encrypted.

1.074 If a secure server is being employed as a “drop box,” make sure the information in this “drop box” is erased from the server after it has been downloaded.

1.075 If a secure server is being employed as a “drop box,” access to the drop box should be controlled with strong authentication measures, such as a username and token to access the drop box and then a onetime password, sent by another channel, to access the materials.

1.076 Use a different communication channel for sending the encryption key for the information being sent from the design facility to the wafer mask production facility.

1.077 Use a new encryption key for the physical layout designs of each successive product.

Creation and evaluation of product prototypes

Building of prototypes

1.078 Substitute field programmable gate arrays (FPGA's) for regular components wherever possible in the building of prototypes, not just to save time and money, but also to limit the dissemination of design information.

1.079 Procure the generic components of the prototypes in an anonymous fashion, so that it would be difficult for an outsider to construct a list of which components are being used or to insert compromised components into the production of the prototype.

1.080 Make sure that there is a documented chain of custody, recording the locations, dates, times, and persons responsible for each of the critical prototype components as they are built and brought together for pre-assembly and assembly.

1.081 Do as much as possible of the molding of non-electronic components, the circuit board pre-assembly, and the actual prototype assembly within a facility fully controlled by the product designers.

Testing of prototypes

1.082 Make sure that there is a documented chain of custody, recording the locations, dates, times, and persons responsible for each completed prototype, as it is moved to different rooms or facilities in the course of the various testing procedures.

1.083 Allow only authorized personnel to have access to the prototypes, including those that are not going into production.

1.084 Document the identities, times, and circumstances of anyone accessing the prototype(s).

1.085 Include simulations of intentional attacks with the performance tests and durability tests to which the prototypes are subjected.

1.086 Make sure the test results from the prototype(s), especially the performance data, are stored and communicated in secure ways.

1.087 Take special precautions to secure the defect and vulnerability data from the prototype(s) and to limit those with access to it.

1.088 When alternative prototypes are being tested, withhold all clues as to which prototype will actually be put into production.

1.089 Destroy the obsolete prototypes in a carefully specified manner that prevents any information from being retrieved from them.

Transmission of prototype samples for production quotes

1.090 Starting the actual prototypes and prototype components, select or construct prototype samples specifically for the purpose of obtaining production quotes.

1.091 If it can be readily done, remove or modify any revealing aspects of the prototype samples that aren't necessary for producing the production quotes.

1.092 Estimate the degree of harm that would be caused by each prototype sample falling into the wrong hands prior to the start of production.

1.093 If having a given prototype sample fall into the wrong hands could cause great harm, arrange for it to be transported only by trusted couriers, operating in pairs.

1.094 If a pair of trusted couriers are employed, make sure each is equipped with a personal GPS device and makes regular radio or cell phone contact.

1.095 Seal each prototype sample for shipping with tamper-revealing seals and lock it in a sturdy transport box.

1.096 Have two personnel at the destination facility verify that they have received the prototype sample with its transport box and tamper-revealing seals intact.

1.097 Limit the information that will be sent to supplement the prototype examples to that which is actually necessary for the production quotes.

1.098 Transmit the supplementary information corresponding to the prototype samples in an encrypted form and over a virtual private network (VPN).

1.099 Use a different communication channel for sending the encryption key for the supplementary information corresponding to the prototype samples.

1.100 Verify that the prototype samples are sent back using the same sort of security measures as when they were sent out.

1.101 Make sure that each prototype sample is returned complete, after the production quotes have been prepared, but before they have been accepted or rejected.

1.102 If the prototype samples are not going to be used again, make sure that they are securely destroyed.

Creation of templates and molds for the non-electronic components

1.103 Make sure the designs for the templates and molds for the non-electronic components, especially the component housings, take full account of the ways the final components might differ in size from the prototype components, so that extra spaces aren’t created that would make illicit add-ons easier.

1.104 Use coded labeling for templates and molds, so that the labels do not reveal where and how the corresponding components are going to be used.

1.105 If the production of templates and molds is outsourced, arrange for them to be sent, along with test examples, to the design facility for detailed inspection before being forwarded to the production facilities.

1.106 Send the templates and molds directly from the design facility to the facilities where they are going to be used in the production of the non-electronic components.

Consolidation and clean-up of design process information

1.107 Have a small team from the corporation that owns the designs verify that the corporation has copies of all the key designs and simulation data from each stage of the design process, along with adequate explanatory notes.

1.108 As soon as it is clear that the designs will not need to be revised further and their receipt by their owner is verified, initiate a program of systematically expunging the design data from each facility used to produce the designs.

1.109 Have two information technology specialists from each design facility compile a complete list of all the places in the facility where design data might still reside, including any temporary and backup documents that might have been automatically generated by the computers used in the design process.

1.110 Have an information technology specialist from each design facility, accompanied by a senior supervisor or a representative of the designs' owner, perform a thorough wipe of the design data at each digital location where it might reside.

1.111 Have the information technology specialist and supervisor or representative who witnessed the data being wiped personally sign a declaration that this was done and that no further data on that product's designs reside in the facility's information systems.

1.112 Send a copy of each document testifying that the design data was wiped to the team responsible for the consolidation and clean-up of the design data.

1.113 Have all of the people who worked on the designs collect all of the paper notes, diagrams, and print-offs they used in the design process and forward them in sealed packages to the team responsible for the consolidation and clean-up of the design data.

1.114 Have the team responsible for the consolidation and clean-up of the design data verify that all the documents and data that were likely to have been created during the design process have been accounted for and dealt with properly.

2. The Photomask Production Phase

Wafer mask receiving

Receiving of mask specifications and layouts

2.001 Severely limit the personnel allowed to access the computers used to receive and handle the mask specifications and layouts.

2.002 Require two-factor authentication for any access to the computers used to receive and handle the mask specifications and layouts.

2.003 Require two authorized personnel to be present whenever sets of mask specifications and layouts are being accessed or processed.

2.004 Maintain regular logs recording which personnel access the mask specifications and layouts and at what times.

2.005 For the reception of mask data, either: a) provide a connection employing an encrypted, virtual private network (VPN) that allows direct instruction of the machines writing the masks; or b) download the mask specifications and layouts through an encrypted connection with a secure server that is being employed as a "drop box."

2.006 Allow no backup copies of the mask specifications and layouts at the wafer mask production facility.

2.007 If any mask data needs to be reloaded, apply to the design facility that provided it, so that a second secure transmission of the data can be arranged using the same procedures that were followed the first time.

Receiving of materials and equipment for wafer mask production

2.008 Store incoming supplies in locked storage cages, or locked storage rooms under constant video surveillance, that are each accessible only by two people together.

2.009 If possible, arrange for the storage cages or storage rooms to be only opened by the simultaneous application of two keys or biometric identifiers to two electronic locks that are physically beyond the reach of a single person.

2.010 Make sure that the view into the storage cages is unobstructed or that the video feed from the storage rooms is constantly monitored, so that activity inside the storage areas or changes in their contents are immediately visible.

2.011 Record each transfer of supplies from the storage cages or storage rooms to the wafer mask production areas, noting the identity or type of supplies, the quantity, the time, and the two people making the transfer.

2.012 Compare the types and quantities of supplies leaving the storage cages or storage rooms to the outputs of the wafer mask production facility to make sure that the quantities of outputs account for the quantities of supplies consumed.

3.013 Verify that any new equipment for the wafer mask production facility has been sent directly from the original manufacturer with tamper-revealing seal intact and with no unexplained delays or detours in its transport.

2.014 Have two trusted personnel oversee the moving and installation of equipment into the wafer mask production facility, maintaining continual, personal surveillance of the personnel carrying out this work.

2.015 Make sure any equipment from the wafer mask production facility that is being replaced and that can store information has any information it might contain securely wiped or removed.

Wafer mask production process

Wafer mask production facility physical layout and work processes

2.016 Make sure the fences, walls, and windows of the wafer mask production facility provide adequate barriers to physical intrusions.

2.017 Make sure the wafer mask production facility has only one entrance and exit in normal use.

2.018 Equip the main entry and exit with a mantrap door.

2.019 Equip emergency exits with alarms and video surveillance.

2.020 Limit the personnel with access to the wafer mask production facility to those who genuinely need to be there.

2.021 Use two or three factor authentication (e.g., photo RFID and fingerprint) for all personnel entering and leaving the mask production facility.

2.022 Document the arrivals and departures of all personnel entering the wafer mask production facility.

2.023 Plan the layout and work flow in the mask production facility so that no single person will have access to any complete set of masks.

2.024 Label the masks in ways that do not reveal the sequence in which they will be applied during production.

2.025 Make sure multiple complementary masks are not subjected to repair with standard repair tools operated by the same personnel.

2.026 Arrange for random, unannounced access to the wafer mask production facility by the corporate customer or a trusted third party for inspection purposes.

Wafer mask production facility information processes

2.027 Make sure the network for the wafer mask production facility is isolated from other corporate networks.

2.028 Carry out all non-technical operations using the corporate network that is kept outside the secure rooms that are used for wafer mask production.

2.029 Make sure the wafer mask production area has no more than one access point to the internet.

2.030 Utilize non-standard, higher-number ports for the special communications coming into the wafer mask production facility.

2.031 Arrange for the firewalls though which incoming data must pass to block all types of communications and all logical ports, except those required for the main tasks of the facility.

2.032 Set the access controls in the wafer mask facility's information systems so that they only allow an employee to access the systems and data deemed necessary for that employee's work assignment.

2.033 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

2.034 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

2.035 Maintain regular logs recording which personnel access which systems and data and at what times.

2.036 Allow the network for the wafer mask production facility to be accessed only by "thin client" terminals that are not running any software applications of their own.

2.037 Physically disable all the open physical data ports on the "thin client" terminals and other equipment, so that portable memory devices cannot be plugged into them.

2.038 Track all access and distribution of the mask specifications and layouts using an automated system.

2.039 Arrange for any abnormally large downloads of information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

2.040 Make sure there is no device containing information on mask specifications and layouts that could be physically removed from the facility without great difficulty.

2.041 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information used in the wafer mask production facility and, depending what is uncovered, bring appropriate remedial, employment, and/or legal action.

2.042 When the production of a set of wafer masks is finished, perform a secure wipe of all devices containing the data that was used, with two authorized personnel observing the procedure and verifying that it was done correctly.

Wafer mask production personnel

Introduction of personnel to the wafer mask production facility

2.043 Make sure all personnel who will be admitted to the wafer mask production facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

2.044 Require a greater degree of background checks for the personnel who will be involved in the receiving and handling of mask specifications and layouts.

2.045 Require each employee in the wafer mask production facility to sign an agreement specifying that he or she has not retained documents from a previous employer containing trade secrets, confidential data, or other intellectual property.

2.046 Require each employee in the wafer mask production facility to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them, including fellow employees.

2.047 Require each employee in the wafer mask production facility to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

2.048 Require each employee in the wafer mask production facility to sign an agreement specifying that he or she will not solicit or engage in business with the company’s customers or suppliers for at least a year after leaving the company.

2.049 To the extent legally permissible, require each employee in the wafer mask production facility to sign an agreement specifying that he or she will not recruit or hire the company’s employees for at least a year after leaving the company.

2.050 Conduct entrance interviews in which each new employee in the wafer mask production facility confirms his or her understanding that no trade secrets, confidential data, or other intellectual property from previous employers can be used on this new job.

2.051 Explicitly define the limitations on the physical and digital privileges of each employee in the wafer mask production facility.

2.052 Require each employee in the wafer mask production facility to acknowledge the limitations on his or her physical and digital access privileges.

Management of personnel in the wafer mask production facility

2.053 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

2.054 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not from the same family or clan and, where practical, not from the same town or tribe.

2.055 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not kept together as a pair, but are rotated among other partners.

Exclusion of personnel from the wafer mask production facility

2.056 Make sure that any employee discovered to be intentionally removing *any* information from the wafer mask production facility is immediately and permanently denied all access to the facility, unless further access is being intentionally allowed under surveillance as part of a criminal investigation.

2.057 Make sure that an employee's physical and digital access to the wafer mask production facility and its information systems is ended at the same time his or her work responsibilities inside that facility are ended.

2.058 Conduct exit interviews in which anyone who will no longer be employed by the wafer mask production facility confirms his or her understanding that *no* knowledge of trade secrets, confidential data, or other intellectual property acquired or created during work for that facility can be used in future jobs.

Management of finished masks

Storage and disposal of masks

2.059 Make security the major consideration in decisions about when and whether to store the masks at the mask production facility, a bonded storage facility, or some other location, when they are not being used.

2.060 Make sure that the storage vault for the masks is kept locked and that it can only be accessed by two authorized personnel.

2.061 Arrange for conspicuous labels to be promptly placed on any masks that are obsolete, due to being defective, no longer needed, or past the date up to which they need to be stored.

2.062 Use tamper-revealing materials for the labels identifying masks as obsolete.

2.063 Make sure that masks are scheduled for prompt destruction once they have become obsolete.

2.064 Break down the obsolete masks into pieces of a small, specified size when it is time to destroy them.

2.065 Require two authorized personnel to observe and verify the physical destruction of any obsolete masks, or alternatively, ship them to the owner of the intellectual property for destruction.

Shipping of finished masks

2.066 Do not ship the finished masks to the fabrication facility until the fabrication facility is almost ready to install them on the photolithography projectors.

2.067 Divide the masks from each mask set into two different packages that will be shipped separately.

2.068 Make sure that information on the sequence of layers and the specification of intervening processes (job deck view) is not shipped with the finished masks.

2.069 Seal each package for shipping with tamper-revealing seals and lock it in a sturdy transport box, separate from the remainder of the mask set.

2.070 Use transport boxes equipped with GPS and radio tracking.*****

2.071 Use transport boxes that will record when and where they are opened and send a radio signal transmitting this information.*****

2.072 Ship the two packages containing different parts of the same mask set at different times via different vehicles.

2.073 Use two trusted couriers to transport each package of masks to the fabrication facility.

2.074 Make sure each courier is equipped with a personal GPS device and makes regular radio or cell phone contact.

2.075 Vary the schedule and route of the couriers transporting the mask shipments.

2.076 Send the information on the sequence of layers and the specification of intervening processes (job deck view) in an encrypted form and over a virtual private network (VPN).

2.077 Use a different communication channel for sending the encryption key for the information on the sequence of layers and the specification of intervening processes (job deck view).

2.078 Strictly limit the number of newly designed microchips or other electronic components that will have their sequence and process specifications sent using the same encryption key.

3. The Microelectronic Fabrication Phase

Microelectronic fabrication sourcing and receiving

Hand-off of wafer masks and fabrication specifications

3.001 Verify the identity of the delivering couriers with photographs or biometric identifiers transmitted separately, in advance.

3.002 Require two authorized people for accepting a delivery of masks.

3.003 To the extent legally permissible, photograph the two delivering couriers making the hand-off to the two personnel accepting the delivery.

3.004 Document the exact time of the delivery and the non-photographic identifiers of the personnel participating in the hand-off.

3.005 Require two-factor authentication for any access to the computers used to receive and decrypt information on the sequence of layers and the intervening production processes.

3.006 Require two authorized people to be present for receiving and decrypting information on the sequence of layers and the intervening production processes (job deck view).

Sourcing and receiving of fabrication materials and generic parts

3.007 Verify that all materials and parts, including generic ones, are coming from reputable suppliers.

3.008 Require any outside suppliers who cannot be rapidly replaced by other suppliers to report periodically the quantity of future shipments they will be able to make from inventory if their production is interrupted.

3.009 Arrange for automatic customer notifications if the inventories of designated hard-to-replace critical supplies drop below specified levels.

3.010 Store incoming supplies in locked storage cages, or locked storage rooms under constant video surveillance, that are each accessible only by two people together.

3.011 If possible, arrange for the storage cages or storage rooms to be only opened by the simultaneous application of two keys or biometric identifiers to two electronic locks that are physically beyond the reach of a single person.

3.012 Make sure that the view into the storage cages is unobstructed or that the video feed from the storage rooms is constantly monitored, so that activity inside the storage areas or changes in their contents are immediately evident.

3.013 Run quality checks on the material batches shortly after their delivery.

3.014 Tag the supplies and/or identify unique characteristics of the material batches that can be used to track them.

3.015 Record each transfer of supplies from the storage cages or storage rooms to the fabrication areas, noting the identity or type of supplies, the quantity, the time, and the two people making the transfer.

3.016 Compare the types and quantities of supplies leaving the storage cages or storage rooms to the outputs of the fabrication facility to make sure that the quantities of outputs account for the quantities of supplies consumed.

Sourcing, receiving, and installation of microelectronic fabrication equipment

3.017 Make sure all equipment for the fabrication facility is purchased only from trusted suppliers with a transparent corporate identity and a known business history.

3.018 Verify that each piece of equipment for the fabrication facility was sent directly from the supplier with no unexplained delays or detours in the shipping route.

3.019 Require a clear chain of custody for any equipment for the fabrication facility that is not being purchased directly from its manufacturer.

3.020 Verify with the original manufacturer the authenticity of any important pieces of equipment purchased from a third party, even if that third party is considered a trusted supplier.

3.021 Make sure any newly arrived equipment is kept in a locked storage space prior to installation.

3.022 Have each newly arrived piece of equipment inspected inside and out by a trusted expert familiar with such equipment and make sure that the expert can account for the presence and features of each observable component.

3.023 Have two trusted personnel oversee the moving and installation of equipment into the fabrication facility, maintaining continual, personal surveillance of the personnel carrying out this work.

3.024 Make sure any equipment from the fabrication facility that is being replaced and that can store information has any information it might contain securely wiped or removed.

Microelectronic fabrication processes

Physically securing the fabrication facility

3.025 Make sure the fences, walls, and windows of the fabrication facility provide adequate barriers to physical intrusions.

3.026 Make sure the fabrication area has only one entrance and exit in normal use.

3.027 Equip emergency exits with alarms and video surveillance.

3.028 Specify what types of equipment are allowed in the fabrication facility in agreement with the corporate customer.

3.029 Limit the personnel with access to the fabrication facility to those who genuinely need to be there.

3.030 Document the arrivals and departures of all personnel entering the fabrication facility.

3.031 Provide a place outside the fabrication facility, where workers can check their cell phones, music players, pocket knives, and other devices that are not allowed into the facility.

3.032 Scan both *incoming* and outgoing workers for memory devices, wireless transmitters or receivers, digital cameras, counterfeit parts, mechanical tools, and other items that could have improper purposes.

3.033 Arrange for any outside personnel carrying out equipment maintenance or upgrades to be escorted and supervised at all times by a trusted employee familiar with the sort of procedures that are being carried out.

Control of information systems in the fabrication facility

3.034 Make sure the fabrication facility networks are isolated from other corporate networks.

3.035 Compartmentalize the fabrication facility networks, so that each set of equipment has access to no more of the design than necessary.

3.036 Set the access controls in the fabrication facility's information systems so that they only allow an employee to access the systems and data deemed necessary for that employee's work assignment.

3.037 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

3.038 Severely limit the information accessible to equipment maintenance personnel.

3.039 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

3.040 Maintain regular logs recording which personnel access which systems and data and at what times.

3.041 Arrange for any abnormally large downloads of information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

3.042 When the production run is finished, perform a secure wipe of all devices containing the data that was used, with two authorized personnel observing the procedure and verifying that it was done correctly.

Fabrication facility work processes

3.043 Restrict all personnel in the fabrication facility to the physical areas they need to enter in order to carry out their specific job assignments.

3.044 Maintain constant video surveillance of the fabrication processes with high-quality cameras that have the capability of low speed, high quality video playback.

3.045 Separate the masks, so that they are not all accessible at the same place, at the same time.

3.046 Use only automated systems for wafer transport.

3.047 Conceal from the fabrication facility personnel the identities of the customers for all components.

3.048 Arrange for random, unannounced access to fabrication facility for inspections (probably by a trusted third party, who can protect the fabrication facility's intellectual properties from its customer).

3.049 Arrange for environmental quality issues above a specified level or frequency to be automatically reported to the corporate customer.

3.050 Arrange for auditing of the fabrication facility production schedule by the corporate customer or a trusted third party to verify that there weren't any undocumented production runs.

3.051 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information used in the fabrication facility and, depending what is uncovered, bring appropriate remedial, employment, and/or legal action.

Managing the fabrication facility supply inventory

3.052 Track the movement of supplies within the fabrication areas, using automatic scanning wherever possible.

3.053 Arrange for the material inputs of each production run to be automatically reported to the corporate customer, so that yield levels can be verified.

3.054 Make sure that all input ingredients are accounted for across successive production runs to confirm that more components weren't made than reported and that there weren't any undocumented production runs.

3.055 Make sure all defective components that are produced are delivered to the corporate customer or subjected to a documented destruction witnessed by two authorized people.

3.056 Arrange for regular audits at unpredictable times of the supply inventories and of the tracking data on parts and materials.

3.057 Carry out an immediate investigation if there are significant quantities of supplies unaccounted for at any stage and take steps to prevent this from happening again.

Personnel in microelectronic fabrication

Introduction of personnel to the fabrication facility

3.058 Make sure all workers who will be admitted to the fabrication facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

3.059 Require a greater degree of background checks for the personnel who will be allowed in the testing facility or the failure analysis facility.

3.060 Require each employee in the fabrication facility to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them, including fellow employees.

3.061 Require each employee in the fabrication facility to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

3.062 To the extent legally permissible, require each employee in the fabrication facility to sign an agreement specifying that he or she will not solicit or engage in business with the company's customers or suppliers for at least a year after leaving the company.

3.063 Require each employee in the fabrication facility to sign an agreement specifying that he or she will not recruit or hire the company's employees for at least a year after leaving the company.

3.064 Conduct entrance interviews in which each new employee in the fabrication facility attest that he or she has received the above warnings and understands that if he or she disregards these warnings or otherwise does not comply, he or she may be subject to appropriate remedial, employment, legal, or criminal action.

Management of personnel in the fabrication facility

3.065 Explicitly define the limitations on the physical and digital privileges of each employee.

3.066 Require each employee to acknowledge the limitations on his or her physical and digital access privileges.

3.067 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

3.068 Where local conditions permit, make sure that the fabrication work force contains at least a few people, scattered across various positions, who are not from the same clan, town, or tribe, and who have worked for the firm less than three years, so that improper collusion between workers is made more difficult.

3.069 Make sure that there are regular rotations of fabrication facility supervisory personnel, so that the same supervisor does not spend many weeks in the same physical position with the same responsibilities.

3.070 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not consistently from the same family or clan and, where practical, not from the same town or tribe.

3.071 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not kept together as a pair, but are rotated among other partners.

Exclusion of personnel from the fabrication facility

3.072 Make sure that any employee discovered to be intentionally removing *any* information from the fabrication facility is immediately and permanently denied all access to the facility, unless further access is being intentionally allowed under surveillance as part of a criminal investigation.

3.073 Make sure that an employee's physical and digital access to the fabrication facility and its information systems is ended at the same time his or her work responsibilities inside the facility are ended.

3.074 Conduct exit interviews in which anyone who will no longer be employed by the fabrication facility attest that he or she has received the warnings described in sections 3.060 through 3.064 and understands that if he or she disregards these warnings or otherwise does not comply, he or she may be subject to appropriate remedial, employment, legal, or criminal action.

Microelectronic fabrication quality control and verification tests

Routine quality testing

3.075 Adjust the frequency and severity of the quality controls, depending on the criticality of the intended product.

3.076 Keep all test equipment in a locked space or cabinet when it is not in use.

3.077 Require two authorized personnel to be present in order to unlock the space or cabinet in which the test equipment is kept.

3.078 Limit all knowledge of the specific test procedures to the few test personnel with a genuine need-to-know.

3.079 Carry out the tests using test programs that are running only on a secure test server.

3.080 Make sure the network connection with the secure test server is itself secure with encryption of all test data transmissions.

3.081 Prevent the test personnel from having any access to the test programs, apart from the test data inputs.

3.082 Limit access to the equipment for wafer probing (to make sure the probing equipment isn’t used to sabotage the wafers).

3.083 Collect and secure raw data on the use of the wafer probing equipment (for audit purposes).

3.084 Erase the test data and test programs as soon as the production run for that microchip is finished, the chips have been mounted, and the finished components have been packaged for shipping.

Failure analysis and reliability testing

3.085 Physically segregate the failure analysis center from the fabrication space.

3.086 Severely limit the personnel with access to the failure analysis center.

3.087 Document the arrivals and departures of any personnel entering the failure analysis center.

3.088 Map out a strategy for failure analysis that allows the necessary tests and comparisons to be made with as few documents as possible being simultaneously accessed.

3.089 Automatically track and document the person, place, and time involved in any accessing of documents for failure analysis.

3.090 Do not allow the failure analysis team members to have simultaneous access to the designs, masks, sequence of layers, specification of intervening processes, and product information.

3.091 Erase all copies of the documents used in failure analysis from the computers used in the analysis, as soon as these documents have been used for a given piece of modeling or comparison, even if this means having to retrieve them later from their source.

3.092 If the failure analysis is outsourced to a third party failure analysis lab, make sure that their security procedures are at least as stringent as the security procedures for testing and analysis done in-house.

3.093 Report the results of the failure analysis to the design team and to the customer, so that any patterns of failure that might indicate security problems can be identified.

3.094 Report the practical conclusions from the failure analysis to the relevant facility manager as well as to the manager responsible for the specific process that was deemed to be at fault.

Chip package assembly and downloading of firmware

Mounting on chip carrier

3.095 If the mounting of the chips is carried out in a separate physical facility from the fabrication of the chips, arrange for a secure transfer of the unmounted chips, with the chips under constant guard by two trusted personnel.

3.096 Visually inspect the mounted chips before they are encapsulated, in addition to any electronic tests planned or already carried out.

Encapsulation in ceramic, epoxy resin, or other plastic

3.097 Verify that resin ingredients are being added in the right proportions by putting an automated gauge and recorder on their storage reservoirs.

3.098 Make sure the encapsulation process is resulting in chips with a flawless, uniform appearance.

3.099 If possible, use an encapsulation material with distinctive optical properties.*

Downloading of firmware

3.100 If possible, download the firmware for the chip directly from a server owned and maintained by the corporate customer, so that no copies of the firmware are stored in the fabrication facility.

3.101 Make sure the electronic equipment used to download the firmware is isolated from all other networks, except, possibly, for one secure connection to a server owned and maintained by the corporate customer.

3.102 If the firmware is a source of intellectual property control or a repository of highly sensitive information, carry out the downloading of firmware at a separate unit run by the corporate customer.

3.103 Run chip functionality tests after the burn-in of the firmware.

Shipping of microelectronic components

Arrangements for microelectronic component shipments

3.104 Do not store the finished microelectronic components any longer than is necessary to accumulate the quantity included in a standard shipment.

3.105 Verify that the prospective shipping company has a reputation for reliability and integrity and, if appropriate, has been accredited by the relevant authority.

3.106 Use a high-volume shipping company or a variety of shipping companies.

3.107 Ship using a receiving depot that handles many other kinds of shipments, including low value ones.

3.108 To the extent legally permissible, make the packaging and labeling anonymous, so that the nature and contents of the shipments cannot be easily identified while they are in transit.

3.109 Use addresses that appear to go to different destinations for different shipments.

3.110 Use a variety of different outside package shapes and sizes.

Packaging and tracking of microelectronic component shipments

3.111 Package the electronic components in secure containers with tamper-revealing seals.

3.112 Put labels on the containers that can be automatically read (RFID's, UID's, PPID's, or, at least bar codes) and that cannot be removed without causing conspicuous damage to the shipment.

3.113 Require that the containers be scanned and their locations reported, each time they are unloaded from a transport vehicle or loaded into one.

4. The Circuit Board Fabrication Phase

Sourcing and receiving of circuit board materials

Sourcing and receiving of materials and generic parts

4.001 Verify that all materials and parts, including generic ones, are coming from reputable suppliers.

4.002 Require any outside suppliers who cannot be rapidly replaced by other suppliers to report periodically the quantity of future shipments they will be able to make from inventory if their production is interrupted.

4.003 Arrange for automatic customer notifications if the inventories of designated hard-to-replace critical supplies drop below specified levels.

4.004 Store incoming supplies in locked storage cages, or locked storage rooms under constant video surveillance, that are each accessible only by two people together.

4.005 If possible, arrange for the storage cages or storage rooms to be only opened by the simultaneous application of two keys or biometric identifiers to two electronic locks that are physically beyond the reach of a single person.

4.006 Make sure that the view into the storage cages is unobstructed or that the video feed from the storage rooms is constantly monitored, so that activity inside the storage areas or changes in their contents are immediately evident.

4.007 Run quality checks on the material supplies shortly after their delivery.

4.008 Tag the supplies and/or identify unique characteristics of the material batches that can be used to track them.

4.009 Record each transfer of supplies from the storage cages or storage rooms to the circuit board fabrication areas, noting the identity or type of supplies, the quantity, the time, and the two people making the transfer.

4.010 Compare the types and quantities of supplies leaving the storage cages or storage rooms to the outputs of the circuit board fabrication facility to make sure that the quantities of outputs account for the quantities of supplies consumed.

Sourcing and receiving of circuit board fabrication equipment

4.011 Make sure all equipment for the circuit board fabrication facility is purchased only from trusted suppliers with a transparent corporate identity and a known business history.

4.012 Verify that each piece of equipment for the circuit board fabrication facility was sent directly from the supplier with no unexplained delays or detours in the shipping route.

4.013 Require a clear chain of custody for any equipment for the circuit board fabrication facility that is not being purchased directly from its manufacturer.

4.014 Verify with the original manufacturer the authenticity of any important pieces of equipment purchased from a third party, even if that third party is considered a trusted supplier.

4.015 Make sure any newly arrived equipment is kept in a locked storage space prior to installation.

4.016 Have each newly arrived piece of equipment inspected inside and out by a trusted expert familiar with such equipment and make sure that the expert can account for the presence and features of each observable component.

4.017 Have two trusted personnel oversee the moving and installation of equipment into the circuit board fabrication facility, maintaining continual, personal surveillance of the personnel carrying out this work.

4.018 Make sure any equipment from the circuit board fabrication facility that is being replaced and that can store information has any information it might contain securely wiped or removed.

Receiving and tooling of circuit board designs

Organization of the circuit board fabrication layout shop

4.019 Maintain a circuit board layout shop that is isolated from the rest of the circuit board fabrication facility.

4.020 Severely limit the personnel with access to the circuit board layout shop.

4.021 Document the arrivals and departures of any personnel entering the circuit board layout shop.

4.022 Do not allow any employee to be inside the circuit board layout shop unless another employee is also present.

4.023 Make sure the network for the circuit board layout shop is isolated from other corporate networks and from the network for the rest of the circuit board fabrication facility.

Receiving of circuit board specifications and layouts

4.024 Arrange to have the circuit board specifications and layouts transmitted directly to the circuit board layout shop.

4.025 Arrange to receive the circuit board specifications and layouts via a virtual private network (VPN) with an additional encryption of the layout data.

4.026 Arrange to receive the encryption key via a different communication channel.

Creation of the tooling for circuit board layout

4.027 Label the tooling components in such a way that the labels do not reveal the customer or use of the boards being built.

4.028 Make sure each human operation in the application of the circuit board layout software is verified or reviewed by two separate people.

4.029 Make sure the operation of the laser photo-plotters is verified or reviewed by two separate people.

4.030 Divide the layer images, drilling layouts, and other tooling components into different groups, so that they can be transferred to the fabrication facility separately and installed on the fabrication equipment by different personnel.

4.031 Sign each group of tooling components over to a different pair of personnel who will be responsible for installing them on the equipment in the circuit board fabrication facility.

Circuit board fabrication processes

Physically securing the circuit board fabrication facility

4.032 Make sure the fences, walls, and windows of the circuit board fabrication facility provide adequate barriers to physical intrusions.

4.033 Make sure the circuit board fabrication facility has only one entrance and exit in normal use.

4.034 Equip emergency exits with alarms and video surveillance.

4.035 Limit the personnel with access to the circuit board fabrication facility to those who genuinely need to be there.

4.036 Document the arrivals and departures of all personnel entering the circuit board fabrication facility.

4.037 Provide a place outside the circuit board fabrication facility, where workers can check their cell phones, music players, pocket knives, and other devices that are not allowed into the facility.

4.038 Scan both *incoming* and outgoing workers for memory devices, wireless transmitters or receivers, digital cameras, counterfeit parts, mechanical tools, and other items that could have improper purposes.

4.039 Arrange for any outside personnel carrying out equipment maintenance or upgrades to be escorted and supervised at all times by a trusted employee familiar with the sort of procedures that are being carried out.

Control of information systems in the circuit board fabrication facility

4.040 Set the access controls in the circuit board fabrication facility's information systems so that they only allow an employee to access the systems and data deemed necessary for that employee's work assignment.

4.041 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

4.042 Severely limit the information accessible to equipment maintenance personnel.

4.043 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

4.044 Maintain regular logs recording which personnel access which systems and data and at what times.

4.045 Arrange for any abnormally large downloads of information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

4.046 When the production run is finished, perform a secure wipe of all devices containing the data that was used, with two authorized personnel observing the procedure and verifying that it was done correctly.

Management and oversight of the circuit board fabrication operations

4.047 Maintain constant video surveillance of the circuit board fabrication processes with high-quality cameras that have the capability of low speed, high quality video playback.

4.048 Keep the personnel throughout the circuit board fabrication facility from knowing how and where each batch of boards is going to be used.

4.049 Make sure personnel do not have physical access to the circuit board fabrication equipment during their breaks.

4.050 Arrange for random, unannounced access to the circuit board fabrication facility by the corporate customer or a trusted third party for inspection purposes.

4.051 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information used in the circuit board fabrication facility and, depending what is uncovered, bring appropriate remedial, employment, legal and/or criminal action.

Managing the circuit board fabrication supply inventory

4.052 Track the movement of supplies within the circuit board fabrication areas, using automatic scanning wherever possible.

4.053 Arrange for regular audits at unpredictable times of the supply inventories and of the tracking data on parts and materials.

4.054 Carry out an immediate investigation if there are significant quantities of supplies unaccounted for at any stage and take steps to prevent this from happening again.

Circuit board fabrication personnel

Introduction of personnel to the circuit board fabrication facility

4.055 Make sure all workers admitted to the circuit board fabrication facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

4.056 Require a greater degree of background checks for the personnel who will be allowed in the circuit board layout shop or in the circuit board testing facility.

4.057 Require each employee in the circuit board fabrication facility to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them, including fellow employees.

4.058 Require each employee in the circuit board fabrication facility to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

4.059 Require each employee in the circuit board fabrication facility to sign an agreement specifying that he or she will not solicit or engage in business with the company's customers or suppliers for at least a year after leaving the company.

4.060 Require each employee in the circuit board fabrication facility to sign an agreement specifying that he or she will not recruit or hire the company's employees for at least a year after leaving the company.

4.061 Conduct entrance interviews in which each new employee in the circuit board fabrication facility attests to his or her understanding that no trade secrets, confidential data, or other intellectual property from previous employers can be used on this new job.

4.062 Explicitly define the limitations on the physical and digital privileges of each employee.

4.063 Require each employee to acknowledge and attest to the limitations on his or her physical and digital access privileges.

Management of personnel in the circuit board fabrication facility

4.064 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

4.065 Make sure that there are regular rotations of circuit board fabrication facility supervisory personnel, so that the same supervisor does not spend many weeks in the same physical position with the same responsibilities.

4.066 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not consistently from the same family or clan and, where practical, not from the same town or tribe.

4.067 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not kept together as a pair, but are rotated among other partners.

Exclusion of personnel from the circuit board fabrication facility

4.068 Make sure that any employee discovered to be intentionally removing *any* information from the circuit board fabrication facility is immediately and permanently denied all access to the facility, unless further access is being intentionally allowed under surveillance as part of a criminal investigation.

4.069 Make sure that an employee's physical and digital access to the circuit board fabrication facility and its information systems is ended at the same time his or her work responsibilities inside the facility are ended.

4.070 Conduct exit interviews in which anyone who will no longer be employed by the circuit board fabrication facility attest that he or she has received the warnings described in sections 4.057 through 4.063 and understands that if he or she disregards these warnings or otherwise does not comply, he or she may be subject to appropriate remedial, employment, legal, or criminal action.

Circuit board quality control and testing

4.071 Maintain a circuit board testing facility that is isolated from the rest of the circuit board fabrication facility.

4.072 Limit the personnel with access to the circuit board testing facility and document their arrivals and departures.

4.073 Set up a special receiving system for electronic components that may need to be loaded into the boards for testing purposes.

4.074 Carry out tests of the circuit boards using generic components whenever possible, rather than the components that will be used in the actual product.

4.075 Erase the test data and test programs as soon as the production run for that circuit board is finished and all the boards have been packaged and sealed for shipping.

Circuit board shipping

4.076 Verify that the prospective shipping company has reputation for reliability and integrity.

4.077 Package the circuit boards in secure containers with tamper-revealing seals.

4.078 Notify the pre-assembly facility when they can expect the circuit boards to be delivered.

5. The Board Pre-Assembly Phase

Pre-assembly sourcing and receiving

Selection of suppliers in buying process

5.001 Compile and update profiles of potential suppliers.

5.002 Eliminate any gray market suppliers from the list of potential suppliers.

5.003 Identify and track potential spot market suppliers in case it becomes necessary to use them.

5.004 Make sure that only trusted suppliers are used for the critical components, such as processors, chip sets, memory, and downloadable firmware, especially drivers.

5.005 Make sure that suppliers whose security has been less thoroughly verified are used only for non-critical components, such as capacitors and power supplies, and for less critical materials, such as epoxies.

5.006 Require the provenance of generic products to be tracked and documented, stage by stage, until their arrival.

5.007 Contractually specify the level of assurance required of each product from an outside supplier.

5.008 Require any outside suppliers who cannot be rapidly replaced by other suppliers to report periodically the quantity of future shipments they will be able to make from inventory if their production is interrupted.

5.009 Use the data on end-user maintenance problems (supplied by the company responsible for the end product) to identify sources that may be substituting counterfeit or poorer quality components for authentic, high-quality components.

Reception and testing of incoming chips, board bases, parts, and materials

5.010 Check the documentation of the shipment tracking from the fabrication facility to the receiving center, making sure there were no unexplained delays or detours.

5.011 Store incoming supplies in locked storage cages, or locked storage rooms under constant video surveillance, that are each accessible only by two people together.

5.012 If possible, arrange for the storage cages or storage rooms to be only opened by the simultaneous application of two keys or biometric identifiers to two electronic locks that are physically beyond the reach of a single person.

5.013 Make sure that the view into the storage cages is unobstructed or that the video feed from the storage rooms is constantly monitored, so that activity inside the storage areas or changes in their contents are immediately evident.

5.014 Physically inspect the received parts, looking specifically for signs of alterations and substitutions, including details of soldering, resin applications, and alignments that are less regular or less perfect than would be produced by a major production facility.

5.015 Tag the supplies and/or identify unique characteristics of the material batches that can be used to track them.

5.016 Carry out random testing of the customized microchip functions.

5.017 Verify the non-proprietary portions of the microchips, as well as the proprietary ones.

5.018 Test specifically for the sort of delayed effect degradations that could have been intentionally caused.

5.019 Record each transfer of supplies from the storage cages or storage rooms to the pre-assembly areas, noting the identity or type of supplies, the quantity, the time, and the two people making the transfer.

5.020 Arrange for automatic customer notifications if the inventories of designated hard-to-replace critical supplies drop below specified levels.

5.021 Compare the types and quantities of supplies leaving the storage cages or storage rooms to the outputs of the pre-assembly facility to make sure that the quantities of outputs account for the quantities of supplies consumed.

Sourcing and receiving of pre-assembly equipment

5.022 Make sure all equipment for the pre-assembly facility is purchased only from trusted suppliers with a transparent corporate identity and a known business history.

5.023 Verify that each piece of equipment for the pre-assembly facility was sent directly from the supplier with no unexplained delays or detours in the shipping route.

5.024 Require a clear chain of custody for any equipment for the pre-assembly facility that is not being purchased directly from its manufacturer.

5.025 Verify with the original manufacturer the authenticity of any important pieces of equipment purchased from a third party, even if that third party is considered a trusted supplier.

5.026 Make sure any newly arrived equipment is kept in a locked storage space prior to installation.

5.027 Have each newly arrived piece of equipment inspected inside and out by a trusted expert familiar with such equipment and make sure that the expert can account for the presence and features of each observable component.

5.028 Have two trusted personnel oversee the moving and installation of equipment into the pre-assembly facility, maintaining continual, personal surveillance of the personnel carrying out this work.

5.029 Make sure any equipment from the pre-assembly facility that is being replaced and that can store information has any information it might contain securely wiped or removed.

Processes in the pre-assembly facility

Physically securing the pre-assembly facility

5.030 Make sure the fences, walls, and windows of the pre-assembly facility provide adequate barriers to physical intrusions.

5.031 Make sure the pre-assembly facility has only one entrance and exit in normal use.

5.032 Equip emergency exits with alarms and video surveillance.

5.033 Limit the personnel with access to the pre-assembly facility to those who genuinely need to be there.

5.034 Document the arrivals and departures of all personnel entering the pre-assembly facility.

5.035 Provide a place outside the pre-assembly facility, where workers can check their cell phones, music players, pocket knives, and other devices that are not allowed into the facility.

5.036 Scan both *incoming* and outgoing workers for memory devices, wireless transmitters or receivers, digital cameras, counterfeit parts, mechanical tools, and other items that could have improper purposes.

5.037 Arrange for any outside personnel carrying out equipment maintenance or upgrades to be escorted and supervised at all times by a trusted employee familiar with the sort of procedures that are being carried out.

Control of information systems in the pre-assembly facility

5.038 Set the access controls in the pre-assembly facility's information systems so that they only allow an employee to access the systems and data deemed necessary for that employee's work assignment.

5.039 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

5.040 Severely limit the information accessible to equipment maintenance personnel.

5.041 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

5.042 Maintain regular logs recording which personnel access which systems and data and at what times.

5.043 Make sure the pre-assembly production area has no more than one access point to the internet.

5.044 Arrange for any abnormally large downloads of information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

5.045 When the production run is finished, perform a secure wipe of all devices containing the data that was used, with two authorized personnel observing the procedure and verifying that it was done correctly.

Management of pre-assembly facility operations

5.046 Restrict all personnel in the pre-assembly facility to the physical areas they need to enter in order to carry out their specific job assignments.

5.047 Stamp each circuit board with a unique serial number before beginning to add components to it.

5.048 Set a work time schedule for the moving conveyer belt of circuit boards that leaves personnel with no time for mischief.

5.049 Keep the people on the line from knowing how and where the circuit board being loaded is going to be used.

5.050 Make sure personnel do not have physical access to the pre-assembly equipment during their breaks.

Oversight of pre-assembly activities

5.051 To the extent legally permissible, maintain constant video surveillance of the assembly line with high-quality cameras that have the capability of low speed, high quality video playback.

5.052 Set up a system for correlating the video surveillance images with the specific circuit boards being assembled.*

5.053 Arrange for random, unannounced access to the pre-assembly facility by the corporate customer for inspection purposes.

5.054 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information used in the pre-assembly facility and, depending what is uncovered, bring appropriate remedial, employment, and/or legal action.

Managing the pre-assembly facility supply inventory

5.055 Make sure the transfer of supplies from the storage cages or storage rooms in the pre-assembly facility reception area is carried out at a rate that makes it easy to oversee the handling of the supplies.

5.056 Track the movement of supplies and unfinished boards within the pre-assembly production areas, using automatic scanning wherever possible.

5.057 Arrange for the tracking system to generate automatic warnings if there are significant discrepancies between the quantities of supplies and unfinished boards reported at one stage of the pre-assembly process and the quantities reported at other stages.*

5.058 Immediately investigate any unexplained discrepancies in the quantities of supplies and unfinished boards, paying as much attention to extra items as to shortages.

5.059 Arrange for regular audits at unpredictable times of the supply inventories and of the tracking data on parts and materials.

5.060 If significant quantities of supplies are still unaccounted for after an investigation, institute improved surveillance and/or improved tracking to prevent this from happening again.

Testing and repair of loaded circuit boards

5.061 Keep all test equipment in a locked cage or cabinet when it is not in use.

5.062 Require two authorized personnel to be present in order to unlock the cage or cabinet in which the test equipment is kept.

5.063 Download the testing information directly from the corporate customer to the specific on-site computers that are used to carry out the tests of the loaded circuit boards.

5.064 Provide extra testing for loaded boards that are intended as replacements and that won't be going through testing at the assembly stage.

5.065 Physically tag any loaded boards that the tests indicate need repair, so that they are easy to distinguish, if possible indicating with the tags what sort of repairs are required.

5.066 Scan the serial numbers of the boards tagged as needing repair, so that they are provided with special tracking that includes extra monitoring.

5.067 Place loaded boards that need repair into a special storage space adjoining the testing area that can be locked whenever there aren't test personnel in attendance.

5.068 Scan the boards awaiting repair when they are removed from the storage space adjoining the testing area.

5.069 Transfer the boards that need repair in manageable-sized batches to a separate repair area or a separate repair facility where all incoming and outgoing parts and materials can be monitored.

5.070 Track the movement of all replacement parts into the repair area.

5.071 Track the movement of all defective or discarded parts out of the repair area and collect the higher value parts for return or special monitored disposal.

5.072 Verify that the repaired boards are returned for another round of testing when all the repairs have been completed.

5.073 Erase the test data and test programs as soon as the circuit boards in that production run have all been fully loaded with their components and made ready for shipping.

Personnel in pre-assembly

Introduction of personnel to the pre-assembly facility

5.074 Make sure all workers admitted to the pre-assembly facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

5.075 Require a greater degree of background checks for the personnel who will handle testing and quality control.

5.076 Require each employee in the pre-assembly facility to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them, including fellow employees.

5.077 Require each employee in the pre-assembly facility to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

5.078 Explicitly define the limitations on the physical and digital privileges of each employee.

5.079 Require each employee to acknowledge and attest to the limitations on his or her physical and digital access privileges.

Management of personnel in the pre-assembly facility

5.080 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

5.081 Make sure that workers in the pre-assembly facility are not exposed to dangerous levels of toxic substances.

5.082 Make sure that workers in the pre-assembly facility are not under fourteen years old.

5.083 Make sure that there are regular rotations of pre-assembly facility supervisory personnel, so that the same supervisor does not spend many weeks in the same physical position with the same responsibilities.

5.084 Make sure that the workers on the assembly line are periodically reassigned to different positions, so that they do not have the same persons next to them.

5.085 Where local conditions permit, make sure that the pre-assembly work force contains at least a few people, scattered across various positions, who are not from the same clan, town, or tribe, and who have worked for the firm less than three years, so that improper collusion between workers is made more difficult.

5.086 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not consistently from the same family or clan and, where practical, not from the same town or tribe.

5.087 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not kept together as a pair, but are rotated among other partners.

Exclusion of personnel from the pre-assembly facility

5.088 Make sure that any employee discovered to be intentionally removing *any* information from the pre-assembly facility is immediately and permanently denied all access to the facility, unless further access is being intentionally allowed under surveillance as part of a criminal investigation.

5.089 Make sure that an employee's physical and digital access to the pre-assembly facility and its information systems is ended at the same time his or her work responsibilities inside the facility are ended.

Shipping of circuit boards to assembly facility

Packaging and dispatching of loaded circuit board shipments

5.090 Verify that the prospective shipping company has reputation for reliability and integrity.

5.091 Package the loaded circuit boards in secure containers with tamper-revealing seals.

5.092 Put labels on the containers that can be automatically read (RFID’s, PPID’s, or, at least bar codes) and that cannot be removed without causing conspicuous damage to the shipment.

5.093 Require that the containers be scanned and their locations reported, each time they are unloaded from a transport vehicle or loaded into one.

6. The Product Assembly Phase

Assembly sourcing and receiving

Selection of suppliers in buying process

6.001 Compile and update profiles of potential suppliers.

6.002 Eliminate any gray market suppliers from the list of potential suppliers.

6.003 Identify and track potential spot market suppliers in case it becomes necessary to use them.

6.004 Require the provenance of generic products to be tracked and documented, stage by stage, until their arrival.

6.005 Make sure that only trusted suppliers are used for the critical components, such as circuit boards, hard drives, the BIOS, and downloadable firmware, especially drivers.

6.006 Verify the choice of any suppliers of critical components with the corporate customer, especially if there is a prospective change in one of these suppliers.

6.007 Make sure that suppliers whose security has been less thoroughly verified are used only for non-critical components, such as capacitors and power supplies, and for less critical materials, such as epoxies.

6.008 Contractually specify the level of assurance required of each product from an outside supplier.

6.009 Require any outside suppliers who cannot be rapidly replaced by other suppliers to report periodically the quantity of future shipments they will be able to make from inventory if their production is interrupted.

6.010 Use the data on end-user maintenance problems (supplied by the company responsible for the end product) to identify sources that may be substituting counterfeit or poorer quality components.

Reception and testing of incoming boards, parts, and materials shipments

6.011 Check the documentation of the shipment tracking from each pre-assembly facility to the receiving center.

6.012 Verify that the tracking records of the circuit board shipments from a pre-assembly facility do not have any unexplained delays or detours.

6.013 Verify the integrity of the tamper-revealing seals on the shipping containers.

6.014 Store incoming supplies in locked storage cages or storage rooms that are each accessible only by two people together.

6.015 If possible, arrange for the storage cages to be only opened by the simultaneous application of two keys or biometric identifiers to two electronic locks that are physically beyond the reach of a single person.

6.016 Make sure that the view into the storage cages is unobstructed or that the video feed from the storage rooms is constantly monitored, so that changes in their contents or activity inside them is immediately visible.

6.017 Physically inspect the incoming boards and other components, looking specifically for signs of alterations and substitutions, including details of soldering, resin applications, and alignments that are less regular or less perfect than would be produced by a major production facility.

6.018 Verify that all critical components have identifying serial numbers and make sure that these are correctly recorded.

6.019 Carry out random testing of the incoming circuit boards and other critical components.

6.020 Test specifically for the sort of delayed effect degradations that could have been intentionally caused.

6.021 Record each transfer of supplies from the storage cages or storage rooms to the assembly areas, noting the identity or type of supplies, the quantity, the time, and the two people making the transfer.

6.022 Arrange for automatic customer notifications if the inventories of designated hard-to-replace critical supplies drop below specified levels.

6.023 Compare the types and quantities of supplies leaving the storage cages or storage rooms to the outputs of the assembly facility to make sure that the quantities of outputs account for the quantities of supplies consumed.

Sourcing and receiving of assembly equipment

6.024 Make sure all equipment for the assembly facility is purchased only from trusted suppliers with a transparent corporate identity and a known business history.

6.025 Verify that each piece of equipment for the assembly facility was sent directly from the supplier with no unexplained delays or detours in the shipping route.

6.026 Require a clear chain of custody for any equipment for the assembly facility that is not being purchased directly from its manufacturer.

6.027 Verify with the original manufacturer the authenticity of any important pieces of equipment purchased from a third party, even if that third party is considered a trusted supplier.

6.028 Make sure any newly arrived equipment is kept in a locked storage space prior to installation.

6.029 Have each newly arrived piece of equipment inspected inside and out by a trusted expert familiar with such equipment and make sure that the expert can account for the presence and features of each observable component.

6.030 Have two trusted personnel oversee the moving and installation of equipment into the assembly facility, maintaining continual, personal surveillance of the personnel carrying out this work.

6.031 Make sure any equipment from the assembly facility that is being replaced and that can store information has any information it might contain securely wiped or removed.

Product assembly processes

Physically securing the assembly facility

6.032 Make sure the fences, walls, and windows of the product assembly facility provide adequate barriers to physical intrusions.

6.033 Make sure the product assembly area has only one entrance and exit in normal use.

6.034 Equip emergency exits with alarms and video surveillance.

6.035 Limit the personnel with access to the assembly facility to those who genuinely need to be there.

6.036 Document the arrivals and departures of all personnel entering the assembly facility.

6.037 Provide a place outside the product assembly facility, where workers can check their cell phones, music players, pocket knives, and other devices that are not allowed into the facility.

6.038 Scan both *incoming* and outgoing workers for memory devices, wireless transmitters or receivers, digital cameras, counterfeit parts, mechanical tools, and other items that could have improper purposes.

6.039 Arrange for any outside personnel carrying out equipment maintenance or upgrades to be escorted and supervised at all times by a trusted employee familiar with the sort of procedures that are being carried out.

Control of information systems in the assembly facility

6.040 Set the access controls in the assembly facility’s information systems so that they only allow an employee to access the systems and data deemed necessary for that employee’s work assignment.

6.041 Limit supervisors’ digital privileges, especially their ability to access and alter any automated logs or activity records.

6.042 Severely limit the information accessible to equipment maintenance personnel.

6.043 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

6.044 Maintain regular logs recording which personnel access which systems and data and at what times.

6.045 Arrange for any abnormally large downloads of information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

6.046 When the production run is finished, perform a secure wipe of all devices containing the data that was used, with two authorized personnel observing the procedure and verifying that it was done correctly.

Management of assembly facility operations

6.047 Restrict all personnel in the assembly facility to the physical areas they need to enter in order to carry out their specific job assignments.

6.048 Exclude any equipment from the product assembly facility that could be used to capture and steal intellectual property, including large and fixed-location equipment.

6.049 Make sure that the contract identification numbers cannot be easily used to identify specific customers.

6.050 Make sure each chassis has a unique product serial number indelibly inscribed on it before beginning to add components to it.

6.051 Make sure that the contract numbers and the identification numbers on the individual product items cannot be used to identify specific customers.

6.052 Prevent the people on the assembly line from learning where the computer or other finished equipment is going from *sources other than* the (anonymous) contract and product numbers.

6.053 Set a work time schedule for the moving conveyer belt of product items being assembled that leaves personnel with no time for mischief.

6.054 Make sure personnel do not have physical access to the assembly equipment during their breaks.

Oversight of assembly activities

6.055 Maintain constant video surveillance of the assembly line with high-quality cameras that have the capability of low speed, high quality video playback.

6.056 Set up a system for correlating the video surveillance images with the specific product items being assembled.

6.057 Scan the video for situations where the assembly line personnel seem to be doing something that doesn’t correspond to their normal work movements and investigate those situations, if necessary inspecting the product items involved.

6.058 Carry out random inspections of product items for signs that components were altered or extra components inserted.

6.059 Arrange for random, unannounced access to the assembly facility by the customer for inspection purposes.

6.060 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information used in the product assembly facility and, depending what is uncovered, bring appropriate remedial, employment, legal and/or criminal action.

Managing the assembly facility supply inventory

6.061 Make sure the transfer of supplies from the storage cages or storage rooms in the assembly facility reception area is carried out at a rate that makes it easy to oversee the handling of the supplies.

6.062 Track the movement of supplies within the assembly areas, using automatic scanning wherever possible.

6.063 Arrange for the tracking system to generate automatic warnings if there are significant discrepancies between the quantities of supplies and unfinished boards reported at one stage of the pre-assembly process and the quantities reported at other stages.*

6.064 Immediately investigate any unexplained discrepancies in the quantities of supplies and partially assembled products, paying as much attention to extra items as to shortages.

6.065 Arrange for regular audits at unpredictable times of the supply inventories and of the tracking data on parts and materials.

6.066 If significant quantities of supplies are still unaccounted for after an investigation, institute improved surveillance and/or improved tracking to prevent this from happening again.

Loading of final firmware and software

6.067 If possible, download the final firmware, the BIOS, drivers, and other pre-installed software directly from a server owned and maintained by the corporate customer, so that no copies are stored in the assembly facility.

6.068 Make sure the electronic equipment used to download the final firmware, the BIOS, drivers, and other pre-installed software is isolated from all other networks, except, possibly, for one secure connection to a server owned and maintained by the corporate customer.

6.069 Specify fully the functions that are to be turned off in order to customize the BIOS.

6.070 Verify by random tests that the appropriate functions were turned off in the BIOS.

6.071 If the customer determines these software programs are sufficiently critical, send product items to a physically separate facility run or supervised by the customer for the reflashing of the bios and the downloading of specialty programs.

6.072 Run chip functionality tests (J-tag ports) after the burn-in of the additional firmware.

Personnel in product assembly

Introduction of personnel to the assembly facility

6.073 Make sure all personnel admitted to the assembly facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

6.074 Require a greater degree of background checks for the assembly facility personnel who will be involved in quality control testing, repairs, the downloading of software or firmware, or post-pack testing.

6.075 Require each employee in the product assembly facility to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them, including fellow employees.

6.076 Require each employee in the product assembly facility to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

6.077 Require each employee in the product assembly facility to sign an agreement specifying that he or she will not engage in business with the company's customers or suppliers for at least a year after leaving the company.

6.078 Require each employee in the product assembly facility to sign an agreement specifying that he or she will not solicit or hire the company's employees for at least a year after leaving the company.

6.079 Conduct entrance interviews in which each new employee in the assembly facility attests to his or her understanding that no trade secrets, confidential data, or other intellectual property from previous employers can be used on this new job.

6.080 Explicitly define the limitations on the physical and digital privileges of each employee.

6.081 Require each employee to acknowledge and attest to the limitations on his or her physical and digital access privileges.

Management of personnel in the assembly facility

6.082 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

6.083 Make sure that workers in the assembly facility are not exposed to dangerous levels of toxic substances.

6.084 Make sure that workers in the assembly facility are not under fourteen years old.

6.085 Make sure that there are regular rotations of assembly facility supervisory personnel, so that the same supervisor does not spend many weeks in the same physical position with the same responsibilities.

6.086 Make sure that the workers on the assembly line are periodically reassigned to different positions, so that they do not have the same persons next to them.

6.087 Where local conditions permit, make sure that the assembly work force contains at least a few people, scattered across various positions, who are not from the same clan, town, or tribe, and who have worked for the firm less than three years, so that improper collusion between workers is made more difficult.

6.088 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not consistently from the same family or clan and, where practical, not from the same town or tribe.

6.089 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not kept together as a pair, but are rotated among other partners.

Exclusion of personnel from the assembly facility

6.090 Make sure that any employee discovered to be intentionally removing *any* information from the product assembly facility is immediately and permanently denied all access to the facility, unless further access is being intentionally allowed under surveillance as part of a criminal investigation.

6.091 Make sure that an employee's physical and digital access to the product assembly facility and its information systems is ended at the same time his or her work responsibilities inside the facility are ended.

6.092 Conduct exit interviews in which anyone who will no longer be employed by the product assembly facility attest that he or she has received the above warnings described in sections 6.075 through 6.081 and understands that if he or she disregards these warnings or otherwise does not comply, he or she may be subject to appropriate remedial, employment, legal, or criminal action.

Product assembly testing and repairs

6.093 Keep all test equipment in a locked cage or cabinet when it is not in use.

6.094 Require two authorized personnel to be present in order to unlock the cage or cabinet in which the test equipment is kept.

6.095 Make sure that testing is automated as much as possible, so that it is more difficult to insert extra components at the testing stage.

6.096 Monitor the activities of the test personnel with extra video surveillance.

6.097 Make sure the testing equipment is locked in read-only mode, so that new instructions cannot be easily added.

6.098 Carry out twenty-four hour functional testing of all servers being assembled at the facility.

6.099 Carry out extensive, but less lengthy testing of all personal computers and other electronic products being assembled.

6.100 Periodically carry out hash-like tests and other design fingerprint tests supplied by the product design team to verify that the product has remained faithful to its design.*

6.101 Physically tag any assembled products that the tests indicate need repair, so that they are easy to distinguish, if possible indicating with the tags what sort of repairs are required.

6.102 Scan the serial numbers of the assembled products tagged as needing repair, so that they are provided with special tracking that includes extra monitoring.

6.103 Place products that need repair into a special storage cage or storage room adjoining the testing area that can be locked whenever there aren’t test personnel in attendance.

6.104 Scan the products needing repair when they are removed from the special storage cage or storage room that adjoins the testing area.

6.105 Maintain a separate repair area or separate facility for repairing assembled products where all incoming and outgoing parts and materials can be readily monitored.

6.106 Make sure the products needing repair are never left unattended when they are being transferred from the storage cage or room adjoining the testing area to the repair area.

6.107 Scan the products that need repair again when they are delivered to the separate repair area.

6.108 Track the movement of all replacement parts or replacement assemblies into the repair area or repair facility.

6.109 Track the movement of all defective or discarded parts out of the repair area and collect the higher value parts for return or special monitored disposal.

6.110 Return any defective pre-assembled components to the facilities that manufactured them.

6.111 Make sure the repaired products are returned for another round of testing when the repairs have been completed.

6.112 Erase the test data and test programs for the product as soon as the production run for that product is finished and all the products that were produced have been made ready for shipping.

Product assembly outputs

Packaging and sealing of products

6.113 Have the keys that reveal which individual product numbers will receive which labels and packaging sent directly to the merge center in an encrypted form.

6.114 Make sure each layer of product packaging is designed and applied in such a way that the packages cannot be readily opened and then resealed without leaving signs that this was done.

Random testing of products after packaging

6.115 Make sure the selection and removal of packaged products for post-pack testing is genuinely random and that the choice of items does not follow any list or schedule made out in advance.

6.116 Carry out the post-pack testing in a cage or room that is physically separate, so that all products, packaging materials, and other items going in and out can be monitored.

6.117 Take extra precautions to make sure that electronic components which could contain malicious firmware are not smuggled into the post-pack testing area.

6.118 Maintain constant video surveillance of the post-pack testing area with high quality cameras.

6.119 Require two personnel to be present for all unpacking, disassembly, inspection, testing, reassembly, and repacking of each assembly product.

6.120 Make a thorough search for unauthorized additions or substitutions of components an important part of the post-pack inspection and testing.

6.121 Verify that the unique serial numbers and other tags on the components are the exact ones that should be present in that assembly product.

6.122 Make sure that the post-pack testing personnel do not let the complete product out of their custody and sight until it is resealed.

Shipping of products

6.123 Make sure that any labels indicating whom the product is for are among the last things added at the merge center.

6.124 Seal the products in bulk shipping containers that have tamper-revealing seals and RFID’s.

6.125 Require that the bulk containers be scanned and their locations reported, each time they are unloaded from a transport vehicle or loaded into one.

7. The Product Distribution Phase

Secure receiving and storage of bulk product shipments

7.001 Check the documentation of each delivery, including the ID of the person making the delivery, and record the delivery data.

7.002 Verify that the tracking records of the container shipments from the assembly facility to the distribution facility do not have any unexplained delays or detours.

7.003 Make sure the space in which the bulk shipment is initially stored is secure.

7.004 Use the data on end-user maintenance problems to identify shipping avenues that may be concealing substandard physical environments or substituting counterfeit products.

Breakdown into individual product orders

Bulk container breakdown and relabeling of product units

7.005 Scan the products at each major stage of processing in the distribution facility, so that their location is always known and recorded.

7.006 Carry out a constant, automated comparison of the bulk shipments entering the facility, the products in the facility, and the products leaving the facility, so that any discrepancies are immediately detected.

Reshipment to middlemen or end users

7.007 Label each shipment with tracking information that cannot be removed without causing conspicuous damage to the shipment.

7.008 Record the handover of products to the re-shipper or transporter, documenting the identities of the personnel on both sides.

Management of product sales force

7.009 Design the advance product descriptions provided to the sales force, so that certain key details about the new product are withheld until the product shipping date.

7.010 If advance samples or mock-up products are going to be provided to the sales force, make sure these have unique serial numbers.

7.011 Require the sales force members to sign for the advance samples or mock-up products and track exactly which sales force members have custody of them at all times.

7.012 Collect the advance samples or mock-up products when the real products become available and verify that all are accounted for.

Management of relationships with middlemen

7.013 Make cooperation with the manufacturer's security measures and security investigations one of the conditions for being an authorized dealer.

7.014 Require authorized dealers to buy the manufacturer's products either directly from the manufacturer or from authorized wholesalers.

7.015 Provide a secure website for customers that makes it easy to find authorized dealers and to check whether a given dealer is an authorized one.

7.016 Carry out joint promotional campaigns with authorized dealers, in order to encourage customers to make their purchases from these authorized dealers.

7.017 Make it easy for dealers to report possible signs of counterfeit products or product tampering and provide them with a sufficient incentive for doing so.

7.018 Require authorized dealers to report the unique serial numbers of any large purchases that were delivered to customers and later returned.

7.019 Provide a system for tracking the provenance of any products that an authorized dealer needs to sell back to wholesalers, especially when the authorized dealer is going out of business.

End-user customer delivery and registration

7.020 Inform end-user customers persuasively of the benefits they will receive from registering the product, allowing updates and upgrades, and providing notification of the product being taken out of service.

7.021 Have end-user customers report a unique product serial number to the product registration website.

7.022 Verify the date of delivery to the end-user customer and the identity of that customer.

7.023 Notify customers immediately if their purchase appears to have been from an unauthorized dealer or if the product they purchased had been previously sold and returned.

8. The Product Maintenance and Disposal Phase

Training of product maintenance personnel

Routine handling of maintenance information

8.001 Withhold intellectual property from maintenance agents who don't need to know it.

8.002 Withhold detailed information about hardware vulnerabilities until remedial measures are being deployed.

8.003 Establish a system for bringing security issues to the attention of security personnel and for making the measures needed to deal with them a high priority.

8.004 If remedial measures cannot be made immediately available to eliminate a security issue, warn maintenance personnel about the symptoms of that security issue.

Advance training for unreleased new products

8.005 Institute strict controls on which personnel have access to the advance training materials.

8.006 Design the advance training, so that certain key details about the new product can be withheld until the product shipping date.

Special training in security issues

8.007 Make security training a requirement for all maintenance personnel, just as mastery of other maintenance procedures is a requirement.

8.008 Require the maintenance personnel to respond *actively* to security training, verifying that they have grasped the key principles involved.

Updates to product

8.009 Offer regular updates or upgrades of final software for free, so that product users have an incentive to check in periodically.

8.010 Make sure that product users can access the upgrades in a secure manner with appropriate verification of electronic certificates.

8.011 Provide the product users with safe and efficient means of testing the upgrades for compatibility, usually by facilitating downloads to test environments.

Servicing of product

Protecting the product user's information and security during maintenance procedures

8.012 Limit the privileges required for remote monitoring and trouble-shooting to those genuinely necessary.

8.013 Provide product users with an easy and secure way of vetting of maintenance personnel.

8.014 Establish maintenance procedures that encourage product users to control strictly the access privileges of the maintenance personnel and to verify that the maintenance personnel are doing what they should.

8.015 Stringently protect any private product user data that must be collected to perform maintenance tasks.

8.016 Do not have the maintenance personnel retain any product user data they collect or access during maintenance procedures unless the customer agrees that the gains to both parties from retaining this information will be greater than the risks.

8.017 Encourage the removal the memory media from any product that is being sent back for repair (and make sure the warranties are written to allow this).

Carrying out secure maintenance and repairs

8.018 Scan both incoming and outgoing maintenance workers to make sure that no potentially insecure or counterfeit components are being brought in and that no authentic components are being improperly removed.

8.019 Record the descriptive label, serial number, and supply source for all replacement parts being brought into the facility where repairs are being performed.

8.020 Verify that any replacement components have gone through the same rigorous supply chain controls and testing as those built into the original product.

8.021 Record the descriptive label and serial number of all parts taken out of the facility where repairs were being performed, including the parts that were damaged and had to be replaced.

8.022 Arrange for the secure destruction or documented recycling of all damaged parts.

8.023 Record the unique serial number of the product being repaired, the type of each major repair, and any replacement parts that were used, and send this information to the company that produced the product.

Protecting end-user customer identities where this is needed for security reasons

8.024 Establish a system of extra-secure maintenance providers who have had special background checks and extra training in the relevant security procedures.

8.025 Have blind-buy end-user customers establish a false-identity enterprise for the administration and billing of support services.

8.026 Have blind-buy end-users with special security needs switch to a secure maintenance provider after purchase, rather than contacting the normal maintenance centers.

Returns for resale or refurbishment

Reception of return shipments from customers and other components

8.027 Authorize each return shipment before it is sent back, noting the reported serial numbers, sales dates, reported condition, reason for return, and amount of credit requested.

8.028 Designate an authorized carrier to transport the return shipment in a reliable and secure manner.

8.029 Make sure the pick up and delivery of the return shipment are recorded, with the exact times and the identities and signatures of the personnel involved in the handovers at each end.

8.030 Maintain a secure area for the unloading and loading of shipments, with video surveillance, high fences, and a secure gate separating the area from outside parking lots and roads.

8.031 Inspect each incoming shipment within twenty-four hours of its arrival to verify that the contents and serial numbers, the physical condition of the equipment, and the condition of any factory equipment seals are exactly as reported.

8.032 Examine the high-value components in each incoming product to verify that they are all present and authentic.

8.033 Inspect the incoming products to verify that no extra electronic components have been added.

8.034 Carefully inspect any additional used parts that are being purchased to make sure that they give every sign of being from authentic branded products and are not counterfeits or inferior substitutions.

8.035 Check the original part numbers and serial numbers of any additional used parts that are being purchased and compare these to the manufacturing records to make sure that there are no inconsistencies that would suggest that the parts are counterfeits.

8.036 If the additional used parts being purchased are from authentic brand-name products, but from another manufacturer, make sure that these parts are from products with an a quality level as high as or higher than the product they will be used to refurbish.

8.037 Make sure that the used parts are of a similar or lower age and have a similar or lower degree of wear than the used products into which they will be installed.

8.038 Store any products or components that are of high value and easy to move in a locked storage cage or a locked room under constant video surveillance.

8.039 Give only a very small number of senior supervisors the ability to unlock the cage or room used to store the products and components that are of high value and easy to move.

8.040 If the returned product is being shipped directly to another customer, re-package it and reseal it in a way that will make it apparent if the product package is opened again before reaching the next customer.

8.041 Provide an extra label on each returned product that will be shipped to another customer, noting that it was opened by a previous customer, re-inspected, and re-sealed.

Management of the refurbishment or re-manufacturing processes

8.042 Make sure the fences, walls, and windows of the re-manufacturing facility provide adequate barriers to physical intrusions.

8.043 Make sure the re-manufacturing facility has only one entrance and exit in normal use.

8.044 Limit the personnel with access to the re-manufacturing facility to those who genuinely need to be there.

8.045 Make sure all personnel admitted to the re-manufacturing facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

8.046 Document the arrivals and departures of all personnel entering the re-manufacturing facility.

8.047 Scan both *incoming* and outgoing personnel for electronic parts and devices.

8.048 Maintain constant video surveillance of the work spaces inside the re-manufacturing facility with high-quality cameras that have the capability of low speed, high quality video playback.

8.049 Severely limit the number of personnel in the re-manufacturing facility who have access to the computer networks used to keep track of the incoming products, the work orders, the inventories on hand, and the outgoing products.

8.050 Track the movement of returned products and critically important replacement components within the re-manufacturing facility, so that their sources, exact nature and features, current locations, and destinations can all be identified at any time.

8.051 Keep the identities of the customers for the re-manufactured products secret from the re-manufacturing facility personnel and store this information separately from the work orders.

8.052 Verify that the quantity of discarded components sent away for recycling exactly matches the quantity of replacement components brought in for the re-manufacturing processes.

8.053 Make sure the testing that the re-manufactured product undergoes before being packed for shipment is not carried out by the same personnel who worked on the product during its refurbishment.

8.054 Use the tracking information on each returned product and on each critically important replacement component to identify the sources of any problems identified in the final testing of the refurbished products.

8.055 Check to make sure that all memory components in the re-manufactured product have been thoroughly wiped of any information that may have been stored in them during previous use.

8.056 Add the shipping labels that identify the customers for the re-manufactured products only after those products are packed, sealed, and ready for shipment.

8.057 Have the encrypted information that reveals which orders go to which customers sent directly to a shipping area computer *after* a designated employee has confirmed that the shipment is ready for shipping.

8.058 Make sure that an employee's access to the re-manufacturing facility is ended at the same time his or her work responsibilities inside the facility are ended.

Disposal of end-of-life-cycle products

Tracking of product disposal by the product manufacturer

8.059 Provide the product user with an incentive to inform the manufacturer when the product is taken out of service.

8.060 Provide the product user with an incentive to return the end-of-life electronic product to a manufacturer’s agent for recycling.

8.061 Make it easy for the product user to provide the manufacturer with the relevant information about the product’s disposal if it is not returned to a manufacturer’s agent for recycling.

8.062 Maintain a centralized product registry, incorporating information about products taken out of service, including the product serial numbers, the date each product was taken out of service, the place and manner of disposal, and the date of disposal.

Management of product disposal by the product end-user

8.063 Inform the manufacturer’s product registry when the product is taken out of service, so that its registration is voided.

8.064 Identify to the manufacturer the intended type of disposal, specifically whether the product is intended for resale, for remanufacturing, or for physical destruction.

8.065 Promptly remove the memory components from any product that is being taken out of service.

8.066 Perform a secure wipe of any memory components from the product being taken out of service and reflash any customized burned-in memory.

8.067 If appropriate, degauss or physically destroy, not just the memory components, but all components that could retain information from their specific use.

8.068 Whenever practical, return the product to a manufacturer's agent for recycling.

8.069 If the product is not being returned to a manufacturer's agent for recycling, remove the manufacturer's trademark and serial numbers from the product.

Recycling of end-of-life products by a manufacturer's agent

8.070 Record exactly what products were returned for re-cycling, both by end-user customers and by other manufacturer facilities, noting the specific serial numbers where available.

8.071 Choose different disposal plans, depending on whether the items being recycled are products in development, outdated products, worn-out products, counterfeit products, or defective products.

8.072 Make sure that all counterfeit products and all products in development that have been sent to the recycling facility are physically destroyed.

8.073 Remove the memory components from the product if the last end-user has not done so.

8.074 Perform a secure wipe of any memory components that are not being physically destroyed and reflash any burned-in memory.

8.075 Carry out random testing of any memory components that are not being physically destroyed to verify that any information they might have contained has been successfully wiped.

8.076 Remove and securely destroy all manufacturer brand labels, serial number plates and stampings, and product casings with distinctive stylings.

8.077 Make sure that the breakdown of any components that will be re-used is complete enough, so that they cannot be resold as branded components.

8.078 Make sure that workers in the recycling facilities are not exposed to dangerous levels of toxic substances.

8.079 Make sure that workers in the recycling facilities are not under fourteen years old.

8.080 Make sure that any components that will be physically destroyed have their constituent materials recycled or disposed of in an environmentally safe manner.

9. The Necessary Legal Conditions

National laws and legal framework

Basic laws and legal principles that need to be operating

9.001 Foreigners and foreign corporations should be able to pursue legal actions, both civil and criminal, on a comparable footing with local citizens and local corporations.

9.002 Information obtained from an analysis of computer logs and other electronic records, as long as they are maintained in the regular course of business and there is a proper chain of custody, should be recognized as competent evidence in court cases.

9.003 The theft of trade secrets, confidential data, or other intellectual property should be recognized as fully comparable to the theft of other valued goods.

9.004 The intellectual properties that an employee produces during work for a corporation should be recognized as belonging to that corporation and not to the employee.

9.005 Employee non-disclosure agreements should be recognized as valid, binding, and enforceable.

9.006 Post-employment restrictions on the use and disclosure of confidential and proprietary information should be recognized as valid, binding, and enforceable.

9.007 Post-employment restrictions on soliciting or engaging in business with a company's customers or suppliers should be recognized as valid, binding, and enforceable.

9.008 Post-employment restrictions on recruiting or hiring the company's employees should be recognized as valid, binding, and enforceable.

9.009 Unauthorized intrusion into the information systems of another organization or person, whether it is accomplished locally or remotely, should be recognized as a criminal offense.

9.010 Unauthorized interception or alteration of confidential communications between information systems should be recognized as a criminal offense.

9.011 The production, sale, or distribution of tools for carrying out unauthorized intrusions into information systems or for intercepting or altering confidential communications between them should be recognized as a criminal offense.

9.012 The willful infringement of copyright, including the copyright of software and data bases, should be recognized as a criminal offense.

9.013 The counterfeiting of electronic components or devices should be recognized as a criminal offense.

9.014 The intentional misrepresentation of electronic devices or software offered for sale, including the substitution of inferior or counterfeit goods, should be recognized as a criminal offense.

9.015 In addition to the direct damage suffered by the purchaser of misrepresented goods, the legal system should recognize the indirect damages suffered by the corporation whose intellectual properties and reputation were being exploited.

Aspects of local laws that could affect security procedures

9.016 There should be sufficient access to financial records, past employment histories, criminal records, and other personal information to make basic background checks possible.

9.017 There should not be restrictions on the videotaping and other surveillance of personnel that would prevent these security measures from being employed effectively inside production facilities.

9.018 The discovery rules in court proceedings should make it possible to prevent the disclosure of trade secrets and other proprietary information, while still allowing enough information access to let a court case go forward without undue handicaps.

The nature of the corporate relationships

General conditions needed to make corporations behave responsibly

9.019 Corporations should be legally required to be truthful in their public accounts, statements, and filings.

9.020 The ownership and control of the corporation should be sufficiently transparent, so that the personal reputations of those responsible for the corporation's policies and activities will suffer if the corporation does not conduct itself properly.

9.021 Corporate officers and senior executives need to be held personally and legally responsible for acts of professional misconduct or negligence while carrying out corporate business.

9.022 The corporation engaging in electronics supply contracts should have enough brand value or other assets at stake, so that its owners would suffer a considerable loss, in proportion to their investment, if the corporation went out of business.

Audit conditions to be included in the supply chain contracts

9.023 The corporate customer needs to have the right to perform security audits of any aspects of production that would not reveal the supplier's trade secrets, business plans, negotiating positions, or other competitively sensitive information.

9.024 In cases where an important security audit *would* reveal the supplier's trade secrets, business plans, negotiating positions, or other competitively sensitive information, the contract should designate a mutually agreed-upon third party to perform the audit.

9.025 Any third parties employed for audits should be contractually held to the strictest security requirement mentioned in the relevant section of these guidelines.

9.026 If the contract is important enough to both the supplier and the corporate customer, arrangements should be made for the corporate customer to have one of its personnel posted in the supplier's production facility as a resident representative.

Financial penalties for security lapses to be specified in the supply chain contracts

9.027 Whenever possible, financial penalties should be contractually agreed upon for failures to comply with contractually specified security measures, similar to the penalties (liquidated damages) that are regularly agreed upon for delivery delays, failure to maintain specified quality levels, and other service shortfalls.

9.028 The financial penalties for security failures should apply regardless of whether the security failure was intentional or whether it resulted in actual damages.

9.029 Some of the security compliance failures that should result in financial penalties include:

- failure to promptly admit inspectors arriving for surprise visits to physical facilities;
- failure to provide prompt and full access to computer logs, access records, task assignments, inventories of parts and materials, and other documents required for contractually specified audits;
- the purchase of parts from gray market suppliers without appropriate provenance, unless, after due diligence, a considered risk management decision, and upon written approval of the first party, it is determined that the parts are required and there are no other suppliers that can provide the required parts with an appropriate provenance;

- failure to adequately control access to the production facility or to the production facility's information system;
- failure to account for parts and materials that were supposed to be tracked.

9.030 International arbitration boards should be contractually agreed upon for determining whether there has been compliance with the contract, what penalties, if any, should be assessed, and how large these penalties should be, given the specifications in the contract.*

Police and criminal courts

Law enforcement operations

9.031 The police should pursue criminals accused of stealing trade secrets, confidential data, and other intellectual property as energetically as they would pursue criminals accused of other white-collar crimes involving similar losses, such as embezzlement.

9.032 The police should pursue criminals accused of crimes against foreigners and foreign corporations as energetically as they would pursue criminals accused of crime against local citizens and local corporations.

9.033 There should be a regular channel by which senior police officials and international business representatives can get to know each other and through which they can arrange for mutual help with the prevention and investigation of crimes affecting electronics manufacturing.

9.034 The police should be receptive to evidence provided by corporations carrying out their own investigations of criminal activities threatening their operations, and the police should be ready to act on that evidence.

9.035 The police should have training in the proper ways to seize, preserve, and examine digital evidence, so that so that it can be used effectively in legal proceedings.

9.036 The police should have the ability, with proper court approval, to seize, copy, and preserve data stored in computer systems owned by or under the control of organizations and persons suspected of criminal offenses.

9.037 The police should have the ability, with proper court approval, to collect traffic data on electronic communications by organizations and persons suspected of criminal offenses and, if appropriate, to intercept, record, and preserve the content of those communications.

9.038 The police should co-operate with international investigations into crimes affecting the production of electronics components and products, including the theft of trade secrets or confidential data, infringement of copyright, and counterfeiting of electronic components and products.

9.039 Judicial officers and prosecutors should be trained in the proper introduction and examination of digital evidence during legal proceedings.

Criminal penalties that need to be applied

9.040 Organizations and persons convicted of criminal acts, such as theft of trade secrets or confidential data, infringement of copyright, counterfeiting, and misrepresentation of items offered for sale, should be required to provide restitution for the damages caused by those criminal acts.

9.041 The courts should recognize that in some cases, a partially suspended sentence and term of probation might be appropriate to enable the organization or person in question to provide greater restitution to those harmed by the crime.

9.042 Organizations and persons convicted of criminal actions, in addition to providing restitution, should be made to suffer a penalty great enough to deter any similar crime. This means that the penalty should be significantly greater than the gains an offender could expect to make from similar crimes before being caught and prosecuted.

9.043 In determining the size of the penalty necessary for deterrence, the scale of the crime should be taken into account, including the amount the organization or person intended to gain by the crime, the amount of damage the organization or person was willing to cause in the commission of the crime, the extent to which the organization or person appears to have habitually pursued or tolerated criminal activity, and the degree to which the organization or person obstructed (or facilitated) the investigation of the crime.

9.044 Remedies should be routinely imposed that limit the continuing harm that could result from the offense and that prevent repetition of the offense.

9.045 Special consideration should be given to any remedies requested by the injured parties.

9.046 Organizations that exist primarily for criminal purposes, if convicted, should be required to pay fines that deprive them of all their assets.

9.047 Serious or repeat offenders found guilty of large thefts of trade secrets, confidential data, or other intellectual property should be eligible for prison terms.

9.048 Serious or repeat offenders found guilty of large scale counterfeiting of electronic components or devices should be eligible for prison terms.

Expert Contributors to This Project

The names in boldface are those who contributed to the final series of workshops and discussions that directly provided material for the drafting of these guidelines. The other names are those who contributed their expertise to the workshops held during earlier phases of this project. The organizational affiliations listed for the contributors are the ones that were current at the time of their participation. *The participation of experts affiliated with these corporations, governmental bodies, and other institutions should not be interpreted as an official endorsement of these guidelines by those organizations.* These experts are listed here to acknowledge the many hours of advice and discussion that most of them contributed to this project and to indicate the range of viewpoints and professional experiences that went into the creation of this document.

Robert Abrams (NJVC)

Mike Ahmadi (GraniteKey)

Nick Akerman (Dorsey & Whitney)

Christina Ayiotis (CSC)

Nadya Bartol (Booz Allen)

Drew Bartkiewicz (Hartford)

Patrica Becker (Northrop Grumman)

Jennifer Bisceglie (Interos)

Joerg Borchert (Infineon)

Stan Borgia (DoE)

Jon Boyens (NIST)

Matt Broda (Nortel)

John Bumgarner (US-CCU)

Brian Callahan (Boeing)

Jeff Carlisle (Lenovo)

John Carter (NSA)

Matt Carpenter (InGuardians)

Thomas Calderwood (Oracle)

Daniel Chen (Mitsubishi)

Larry Clinton (ISA)

Brian Cohen (IDA)

Al Cook (IBSS)

Guy Copeland (CSC)

Jack Danahy (Ounce Labs)

Don Davidson (DoD)

Paul Davis (NJVC)

Thomas Dillon (DoD)

Lawrence Dobranski (Nortel)

David Doughty (Intel)

Mark Duesenberg (Lenovo)

Hossam Elddin Saleem (Universal Motors Agencies)

Kevin Engfer (Northrop Grumman)

Mark Esherick (Siemens)

Jack Farris (Verizon)

Severio Fazzari (Booz Allen)

Vance Fields (Northrop Grumman)

Mohan Ganesan (Satyam Computer Services)

Michael Greelish (Northrop Grumman)

Jeff Givney (Lockheed Martin)

Marc Goodman (Cyber-crime Research Institute)

Werner Gutau (Infineon)

Meg Hardon (Infineon)

Pete Hartigan (Trusted Ventures)

Mike Hickey (Verizon)

James Hoe (CMU)

David Hoffman (Intel)

Richard Howard (iDefense)

Thomas Indelicarto (VeriSign)

Grant Jewell (Northrop Grumman)

Sue Graham Johnston (Oracle)

Stewart Katzke (NIST)

Mike Kennedy (Motorola)

David Lang (Dell)

Thresa Lang (Dell)

Alan Lawrence (Cisco)

Annabelle Lee (NIST)

Karl Levitt (National Science Foundation)

Joshua Magri (ISA)

Tom Mahlik (FBI)

Scott Mansfield (Ericsson)

Richard Marshall (DHS)

John Miller (Intel)

Rama Moorthy (IDA)

Nick Multari (Boeing)

John Nagengast (AT&T)

Michael Nash (IDA)

Thomas Patton (Philips Electronics)

Felipe Paez (Dell)

Gary Phillips (Symantec)

Al Piesco (Lockheed Martin)

Michelle Pinto (Harris)

Sydney Pope (DoD)

Andy Purdy (CSC)

Michael Purdy (Dell)

Cindy Reese (Sun Microsystems, Oracle)

Hart Rossman (SAIC)

Warren Russell (DoD)

Marcus Sachs (Verizon)

Rasoul Safavian (Bechtel Communications)

Tony Sagar (NSA)

Bill Scherlis (CMU)

Mark R. Schiller (HP)

Vishant Shah (DHS)

Stephanie Shankle (Booz Allen)

Ken Silva (Verisign)

Matt Smith (NetApp)

Ken Speck (NSA)

Ken Steinberg (Savant)

Marianne Swanson (NIST)

Andras Szakal (IBM)

Bob Thibadeau (Seagate)

Debbie Turnbull (IBM)

Jun Ueda (Renesas)

Ray Williams (L-3 Communications)

Ben Winter (Lockheed Martin)